3

Monitoring of Wireless Sensor Networks

Benahmed Khelifa[1], Haffaf Hafid[2] and Merabti Madjid[3]
[1]*Béchar University, Algeria, benahmed_khelifa@yahoo.fr*
[2]*University of Es-Sénia Oran, Algeria, haffaf_hafid@yahoo.fr*
[3]*School of Computing & Mathematical Sciences, Liverpool John Moores University, U.K, M.Merabti@ljmu.ac.uk*

1. Introduction

A Wireless Sensor Network consists of small battery powered wireless devices, that are capable of monitoring environmental conditions such as humidity, temperature, noise, etc. Sensor networks do not have a fixed infrastructure but form an ad hoc topology. Wireless sensor networks are emerging as a promising platform that enable a wide range of applications in both military and civilian domains such as battlefield surveillance, medical monitoring, biological detection, home security, smart spaces, inventory tracking, etc. Such networks consist of small, low-cost, resource limited (battery, bandwidth, CPU, memory) nodes that communicate wirelessly and cooperate to forward data in a multi-hop fashion. Thus, they are especially attractive in scenarios where it is infeasible or expensive to deploy a significant networking infrastructure.

In wireless sensor networks, services may fail due to various reasons, including radio interference, de-synchronization, battery exhaustion, or dislocation. Such failures are caused by software and hardware faults, environmental conditions, malicious behavior, or bad timing of a legitimate action. In general, the consequence of such an event is that a node becomes unreachable or violates certain conditions that are essential for providing a service, for example by moving to a different location, the node can no further provide sensor data about its former location. In some cases, a failure caused by a simple software bug can be propagated to become a massive failure of the sensor network. This results in application trials failing completely and is not acceptable in safety critical applications.

The open nature of the wireless communication, the lack of infrastructure, the fast deployment practices, and the hostile deployment environments, make them vulnerable to a wide range of intrusions and security attacks. The motivation for attacking a sensor networks could be, for example, to gain an undeserved and exclusive access to the collected data. There has been a multitude of attacks described in the literature: probabilistic data packet dropping, topology manipulation, routing table manipulation, prioritized data and control packet forwarding, identity falsification, medium access selfishness etc. The protection system of a sensor networks usually relies on the following two mechanisms: (i) authentication and secure protocols and (ii) intrusion and attack (misbehavior) detection. As the experience from the Internet shows, the weaknesses in authentication and secure protocols are frequently exploited. These protocols alone are in general considered being

insufficient to provide the necessary level of protection. Therefore, there has been a lot of effort invested in providing networks with means for a timely detection of an attack or intrusion. Such detection is often based on methods and algorithms known from the field of machine learning.
Additionally, After sensors get deployed in the monitored area, the access to them can be difficult. For example, a sensor network, with the goal to monitor conditions in the sewer system of a large city, might be inaccessible for maintenance, software updates or battery exchange. Therefore, a special focus has been put on designing energy efficient protocols at all layers of the OSI (Open Systems Interconnection protocol stack. Additionally to addressing energy constraints, these protocols should impose a high degree of robustness in order to minimize the need for human intervention.
The use of these sensor networks in hostile environments means that providing quality of service is essential and requires the implementation of fault-tolerant mechanisms that can ensure availability and continuity of service. For example, the maximum coverage of the regions monitored by the network and connectivity of the various nodes of the network must be maintained. However in an environment where each node can fail unexpectedly resulting in the isolation of some parts of the network, this guarantee is neither automatic nor easy to achieve.
For all this problems, the integration of mechanisms for monitoring wireless sensor networks, for the reason of topology control, fault tolerance and security are crucial for the effective use of wireless sensor networks. There are many current management approaches, but each provides only partial solutions to the problems of monitoring and fault tolerance, and they do not adapt to the properties and constraints of many wireless sensor networks.
In summarize there are many papers tried to tackle monitoring methodologies in wireless sensor networks. In this chapter we will try to give an overview on the use of monitoring mechanisms to supervise wireless sensor networks. Then we detailed the description of some research using monitoring mechanisms for reasons of security, topology control or fault tolerance in wireless sensor network, and we will describe our contribution in this field.

2. A survey of monitoring mechanism in WSN

To address these problems , many researchers have used the concept of centralized monitoring, where a control center is responsible for monitoring all network nodes (such as base station, the central controller or manager, and sink) . Other researchers have used a decentralized approach to monitor network nodes as fault detection, security, connectivity and coverage control.

2.1 Monitoring of Connectivity and Coverage in WSN

Connectivity is particularly important for wireless sensor networks. In a wireless sensor network, the deployment strategy often involves using more nodes then necessary and turning off the ones that are not being used for communication or sensing. When the network becomes disconnected, one or more of the redundant nodes can be turned on to repair connectivity [1]. The main problem with this technique is the requirement for extra nodes, and when several nodes in a limited region fail it may no longer be possible to repair

the network. Li and Hou study the problem of adding as few nodes as possible to a disconnected static network so that the network remains connected [2]. They show that the problem is NP-Complete and propose some heuristic solutions. These algorithms require global knowledge of the graph and they are time-consuming to apply. Consequently they are typically not applicable in real-time with dynamic networks.

Using mobility to maintain connectivity has attracted many researchers. The general approach has been the use of mobility to carry data between disconnected components of the network [3]. Another approach is the storage of data when connectivity is disrupted, and sending the data when connectivity is subsequently repaired [4, 5]. A significant problem with these approaches is the latency in data transfer for time critical applications.

K. Benahmed and al. used graph theory and self-organisation mechanism for monitoring connectivity in wirless sensor networks [6].

There are also approaches that can be used to maintain uninterrupted connectivity with dynamic networks. Spanos and Murray propose a technique for providing radio connectivity while moving a group of robots from one configuration to another [7]. However, this analysis is not valid when there are obstacles.

Several other solutions for fault tolerance are based on the nature of redundant sensor networks. Fusion techniques [7, 8] may merge or aggregate the different readings of the sensors. Multi routing paths [9, 21] and techniques to ensure k-connectivity between nodes [10, 11, 12, 13, 14] can be applied to increase the reliability of the transmission of messages in wireless sensors networks.

First, most existing solutions have treated the problems of sensing coverage and network connectivity separately. The problem of sensing coverage has been investigated extensively. Several algorithms aim to find close-to-optimal solution based on global information. Both [22] and [23] apply linear programming techniques to select the minimal set of active nodes for maintaining coverage. More sophisticated coverage model is used to address exposure-based coverage problems in [24][25]. The maximal breach path and maximal support path in a sensor network are computed using voronoi diagram and delaunay triangulation techniques in [24]. The problem of finding the minimal exposure path is addressed in [25]. In [26] , sensor deployment strategies were investigated to provide sufficient coverage for distributed detection. Provided scalability and fault-tolerance, the localized algorithms can be more suitable and robust for large-scale wireless sensor network that operate in dynamic environments. The protocol proposed in [27] uses a local geometric calculation of sponsored sectors to preserve the sensing coverage. However, these protocols do not address the problem of maintaining network connectivity. Several other protocols (e.g., ASCENT [28], SPAN [29], AFECA [30], and GAF [31]) aim to maintain network connectivity, but do not guarantee sensing coverage. Unfortunately, satisfying only coverage or connectivity alone is not sufficient for a sensor network to provide sufficient service. Without sufficient sensing coverage, the network cannot monitor the environment with sufficient accuracy or may even suffer from “sensor voids” where no sensing can occur. Without sufficient connectivity, nodes may not be able to coordinate effectively or transmit data back to base stations. The combination of coverage and connectivity is a special requirement introduced by sensor networks that integrate multi-hop wireless communication and sensing capabilities into a single platform. In contrast, traditional mobile ad hoc networks comprised of laptops only need to maintain network connectivity.

A second limitation of the aforementioned coverage protocols (except for the global algorithm in [22]) is that they can only provide a fixed degree of coverage. They cannot dynamically reconfigure to meet the requirements of different applications and environments, or a same application with varying operational conditions. Finally, while the PEAS [32] protocol was designed to address both coverage and connectivity in a configurable fashion, it does not provide analytical guarantees on the degree of coverage and connectivity. For many critical sensor network applications (e.g., surveillance and structural monitoring) guaranteed degrees of coverage and connectivity are required, and a best effort approach is not sufficient.

2.2 Monitoring Wireless sensor Networks for Security Reason

Wireless sensors networks are vulnerable to many types of attacks. In recent years there have been many proposals using cryptography to ensure secure communication such as SPINS [33], etc. Nevertheless, cryptography alone is not sufficient for node compromise attacks and novel misbehaviors in sensor networks [34].

A protocol called DICAS using local monitoring is proposed by Khalil et al. [35], for secure routing, which mitigates the control and data traffic attacks in sensor networks. They propose a countermeasure for wormhole attacks, called LITEWORP [37], which uses guard nodes to attest the source of each transmission. Neighbor watch [36] is employed by a hop-by-hop resilient packet-forwarding scheme. For reputation and trust based systems, neighbor watch is used as a component to monitor neighborhoods and collect information to build trust relationships among nodes in the network, such as RFSN[38], CONFIDANT[39], CORE[40], etc. For intrusion detection systems, local monitoring is used to build decentralized protocols [41, 42]. Khalil et al. [43] propose a on-demand sleep-wake protocol to shorten the time a node needs to be awake for the purpose of monitoring. They do not, however, consider the optimized selection of monitoring nodes in the network, but focusing on how to schedule nodes to meet the monitoring requirement for given communication links. Hsin et al. [44] propose self-monitoring mechanism, this proposition pay more attention on the system-level fault diagnosis of the network, especially detecting node failures. They do not deal with malicious behaviors as what are considered in the works [36,45,46]. On the other hand, our study emphasizes the optimized node selection for the local monitoring scheme. In [47], the authors present DAMON, a distributed system for monitoring multi-hop mobile networks. DAMON uses agents within the network to monitor network behavior and send collected measurements to data repositories. Zhao et al. [48] propose to scan the residual energy and monitor parameter aggregates including link loss rate and packet count. Such information is collected locally at each node and transmitted back to the sink for analysis. In [49], the authors propose Sympathy tool to actively collect run-time status from sensor nodes like routing table and flow information and detects possible faults by analyzing node status together with observed network exceptions. In [50], an IDS model for ad-hoc networks is presented following the behavioral paradigm. The IDS is decentralized and detection is made by clusters. A technique to safely elect the responsible node for monitoring each cycle was developed. This solution is expensive, thus being inadequate to a WSN. In [51], Marti et al. used Watchdog technique or local monitoring for ad-hoc networks in order to improve the detection of mischievous nodes. It uses a technique called pathrater to help routing protocols to avoid those nodes. In this work, the monitor node watches its neighbors to know what each one of them will do

with the messages it receives from another neighbor. If the neighbour of the monitor nodes changes, delays, replicates, or simply keeps the message that should be retransmitted, the monitor counts a failure. This technique is also used to detect other types of attacks. This approach is not efficient because watchdog needs more memory. If watchdog's neighbor sensors send large number of messages, the watchdog will run out of its memory quickly. However, none of these previous works has sought to give more importance to the election criteria of nodes responsible for monitoring the network. In addition, the audit data used in monitoring and detecting abnormal behavior in the network, does the flow of traffic, but nobody has taken the resources consumed in a sensor as an index of screening abnormalities. The highlight of our work is summarized in a comprehensive strategy for monitoring the network, in order to detect and remove nodes to abnormal behavior. Our work therefore focuses around a strategy of distributed resolution on the algorithmic level, that is to say an implementation of the distributed algorithm throughout the network, in which each sensor involved through local pre-treatment. On the other hand in most of the work, monitoring keys entire population of the sensor network at the same time, this poses a problem of congestion at the communication channel and overloads the sensors responsible for network monitoring. In our case the sensor responsible for monitoring selects and analysis a single sample from the population to monitor.

3. Hybrid Approach for Monitoring the Connectivity and Coverage in Wireless Sensor Networks

The use of sensor networks in hostile environments means that providing quality of service is essential and requires the implementation of fault-tolerant mechanisms that can ensure availability and continuity of service. For example, the maximum coverage of the regions monitored by the network and connectivity of the various nodes of the network must be maintained. However in an environment where each node can fail unexpectedly resulting in the isolation of some parts of the network, this guarantee is neither automatic nor easy to achieve.

The integration of mechanisms for surveillance, topology control and fault tolerance are crucial for the effective use of wireless sensor networks. There are many current management approaches, but each provides only partial solutions to the problems of monitoring and fault tolerance, and they do not adapt to the properties and constraints of many wireless sensor networks. Therefore, the work presented in this paper gives a new approach for monitoring connectivity in wireless sensors networks. We provide a rigorous analysis for the development of fault-tolerance to ensure both ongoing monitoring of network connectivity and self organization, mainly to enhance the degree of connectivity at critical nodes presenting articulation points in the network.

The rest of this sub-chapter is organized as follows. The following sections 3.1 and 3.2 introduce the concepts of connectivity, monitoring and fault tolerance . We model our problem in Section 3.3. Sections 3.4 and 3.5 describe our solution. In Section 3.6, we present our simulation results.

3.1. Connectivity

A network of sensors is considered to be connected only if there is at least one path between each pair of nodes in the network. Connectivity depends primarily on the existence of paths.

It is affected by changes in topology due to mobility, the failure of nodes, attacks and so on. The consequences of such occurrences include the loss of links, the isolation of nodes, the partitioning of the network, the upgrading of paths and re-routing.
Connectivity can be modeled as a graph G (V, E) where V is the set of vertices (nodes) and E the set of edges (links). This graph is said to be k-connected if there are at least k disjoint paths between every pair of nodes u, v ∈ V. Connectivity is a measure of fault tolerance or diversity of paths in the network. The need for 1-connectivity of the network graph is a fundamental condition of it being operational. The connectivity of a network can be expressed as follows [15].

$$\mu(R) = \frac{N.\pi.R^2}{A} \tag{1}$$

where R is the radius of transmission, A the area and N the number of nodes in the area A.
Kleinrock and Silverster have shown that when connectivity μ(R) reaches 6 nodes, the probability that a node is connected tends to 1, i.e. that the network forms a connected graph [14].

3.2. Fault Tolerance

Wireless sensor networks are commonly deployed in hostile environments and are susceptible to numerous faults in several layers of the system. Figure 1 depicts the source of these failures and demonstrates the potential for propagation to higher layers. The source of failures in this classification is divided in to four layers: node, network, sink and the base station.

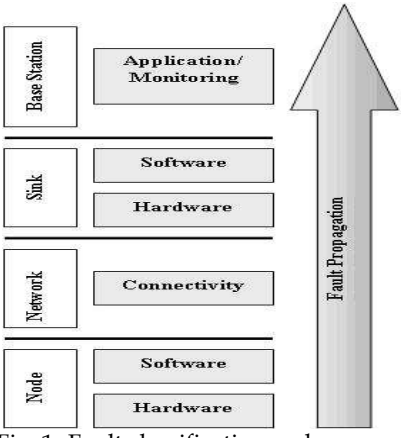


Fig. 1- Fault classification and propagation

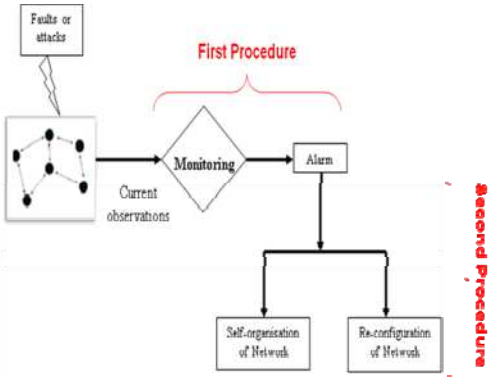


Fig. 2- Monitoring systems

To address these problems it is useful to implement a system that allows monitoring of the network, show figure 2. At any moment such a system must be able to provide the operational status of different devices and to establish mechanisms that provide fault tolerance. By definition fault tolerance [14] is a technique that has been proven to make systems capable of providing a good service, even in the presence of accidental phenomena

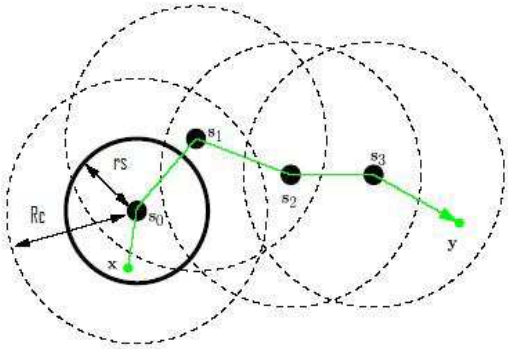
such as disturbance of the environment (external faults), failure of hardware components (internal physical faults), or design faults, particularly software faults (bugs). Under the terms of dependability, faults are the causes of errors, mistakes are part of the abnormal state of the system and when errors are propagated to the system interface – i.e. when the service provided by the system is incorrect – this results in a failure. When mistakes are accidental and sufficiently rare, it is possible to tolerate them. This requires detecting errors before they occur, with error handling in case they can't be rectified. We must also make a diagnosis, in other words identify the fault, isolate faulty components, replace or repair and reset the system in case there is no alternative.
In a wireless sensors network, fault tolerance is the ability to ensure the functionality of the network in the face of any interruption due to failures of sensor nodes.

3.3. Modeling the Problem

In most cases a wireless sensors network can be modelled as a unit graph G (V, E) where V is the set of nodes (with each sensor in the network a vertex in the graph) and E the set of all arcs giving opportunities for direct communication between nodes (we assume that the communication is symmetric, meaning that if a node can hear another, it can also be understood by him). The corresponding graph is undirected. If we set d(u, v) as the physical distance between nodes u and v, and Rc the radius of communication, then E is defined as follows [16, 20].

$$E = \{(u, v) \in V\,2 \mid d(u, v) \leq Rc\} \quad (2)$$

For sensor coverage – i.e. the collection of information by sensors – we need the coverage radius rs, with $Rc \geq 2rs$. Figure 3 shows these two ranges (connectivity and coverage).



x, y are Events — S_i are sensor nodes
R_c is the radio range — r_s is the sensing range

Fig. 3. Connectivity and coverage in wireless sensor network.

3.4. Connectivity Strategy : Our Approach

In this section we will consider methods used for predicting the partitioning of the network. The prediction algorithm acts as a tool to help provide fault tolerance, aimed at improving

the life of the service by detecting critical nodes that might induce a breach of network connectivity should they fail. The mobility of nodes, energy loss, vulnerability to attack and the limited range of their communication implies that the existence of such nodes may result in it becoming impossible to find a route between a source and destination nodes.
The algorithm that we propose for the prediction of partitioning of the network includes the following steps.

- Assess the robustness of the link between nodes.
- If this robustness is below a given threshold, send an alert to self organize the network.

For the assessment of the robustness of communication links, we propose an evaluation based on sets of node-disjoint paths and properties of k-connected graphs.
Theorem (Menger, 1927): In an undirected graph the maximum number of node-disjoint paths from a nonadjacent summit x and summit y is equal to the minimum number of nodes to remove to disconnect x of y [18].
The search for node-disjoint paths between pairs of nodes can be reduced to the search for nodes whose removal disconnects them. Such nodes are called critical points or articulation points and can be detected using a centralized in-depth search algorithm [19]. Figure 4 illustrates this idea.

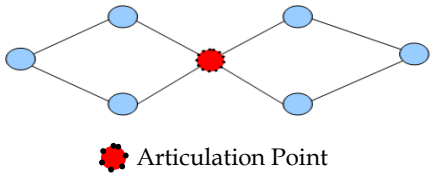


Fig. 4. Topology with an articulation point

Our case is limited to 2-connectivity: we require at least two paths between the source and destination to ensure fault-tolerant connectivity.
Definition 1: A graph is biconnected if for each pair of summits u, v with u ≠ v, there are two summit-disjoint paths that join u and v [20].
Property: A graph is biconnected if and only if it has no articulation point [20].
Algorithm 1: Detection of articulation points in an undirected graph.
Input : G (V, E) Unit Disk Graph
Output : Set of articulation points

- Depth search in graph G and generation of spanning tree T, (in which back edges are shown as dotted lines) to facilitate computing articulation points.
- A vertex x is not an articulation point if it has no successor, or if each of its successor admits a descendant who has a back edge to an ancestor of x in the tree,
- Particular case: the root is an articulation point if it has more than one successor in the tree.

This algorithm has a binomial complexity of the order of O (N + M) for a graph with N vertices and M edges.

3.5 Self Organizing Network

Recent scientific study has considered the behavior of birds, insects and viruses and their capacity to organize themselves. Noting also the pervasive presence and potential benefits of self-organization in natural systems, many researchers have now begun to look at how such models of self-organization can be applied to the design of distributed systems. The mechanisms of self-organization have the potential to provide many solutions in wireless sensor networks. For example, self-organization can be used to change the density of sensor nodes and traffic patterns, or help to reconfigure the network topology in cases where nodes fail or relocate. Inspired by the behavior of ants that organize themselves (moving to form a bridge) and the capabilities of sensors to move or raise their range of connectivity, we propose the following algorithm to allow the self organization of the network, especially around the articulation points discussed above (AP). Our approach is hybrid : content centralized and distributed algorithms . The mechanism for articulation points detection is lunched by the base station, but the self-organisation is lunched by each articulation point. Figure 5 shows this hybrid approach.

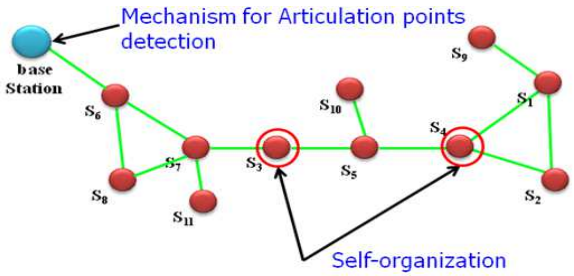


Fig. 5. Hybrid approach for monitoring connectivity in WSN.

Algorithm 2: Self-organization: the principle
Input: G (V, E), with the set of articulation points (AP) previously detected
Output: G (V, E), with a minimum set of articulation points so that G will be at least biconnected.

1. For any articulation point (AP) do
- If there is a neighbour redundant of (AP) then turn on and go to the (AP) following (step 1).
- Else discover the neighbours of (AP) at one hop,
  - If neighbours have redundant nodes, select at least one node with the greatest energy capacity, and move it to the coordinates (x, y) of the (AP) or increase its communication range; go to step 1.
  - Else " no solution at one hop of (AP) "; go to step 1.

End For

This algorithm is demonstrated in the example shown in Figure 6, this algorithm applied to the network to auto-organize and increase connectivity around articulation points.

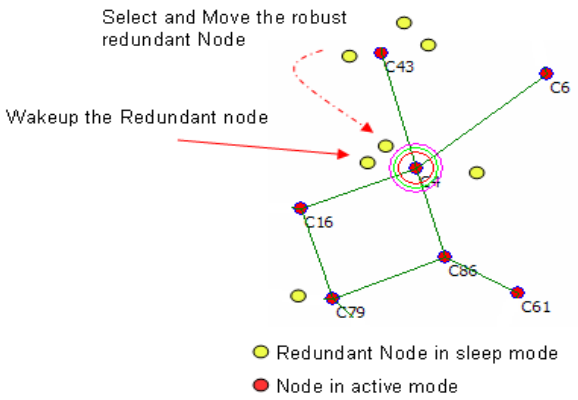


Fig. 6. Self-organization around articulation point

3.6. Simulation and Results

We have tested and validated our algorithm using a simulator implemented in C++, which operates in discrete time. One hundred sensor nodes are distributed randomly on a surface without obstacles. Adjacent nodes at a distance Rc can communicate to form a unit disk graph. The result in figure 7 shows the detection of articulation points (the points surrounded by circles).

A self-organization of the network around the articulation points can increase the degree of network connectivity, the disappearance of the articulation points and finally a fault tolerant network.

We have also simulated the detection of certain targets deployed on the same surface (see figure 10). Consequently any event distant to a sensor with radius r_s will be captured. Figures 11 and 12 give us an idea of the strength of ties between coverage targets. As can be seen in figure 9, every target is covered by at least 2 sensors, ensuring a fault tolerant network. In other words even if some sensors fail there are always other sensors able to provide coverage.

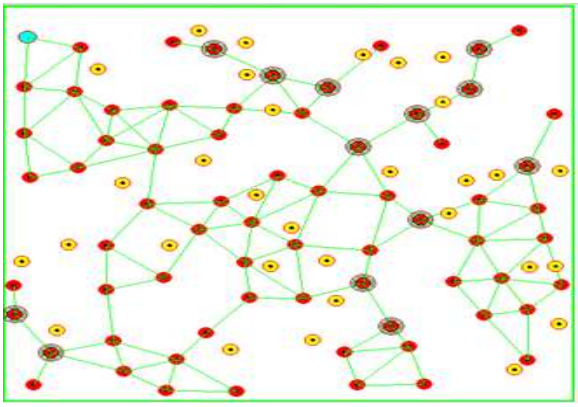
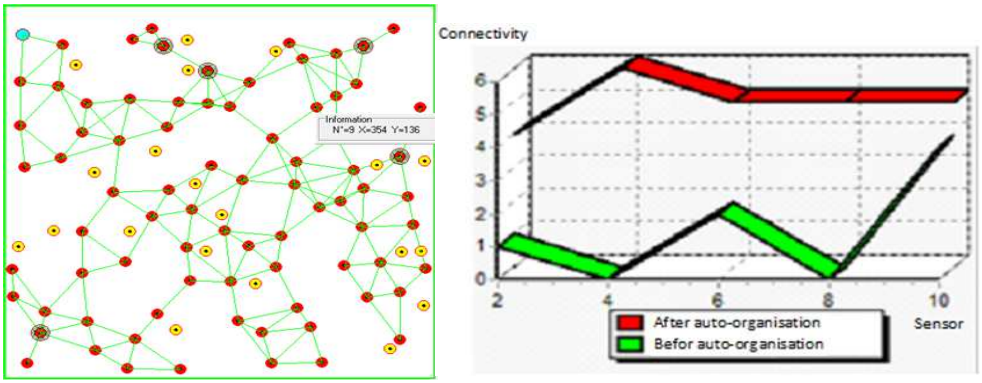


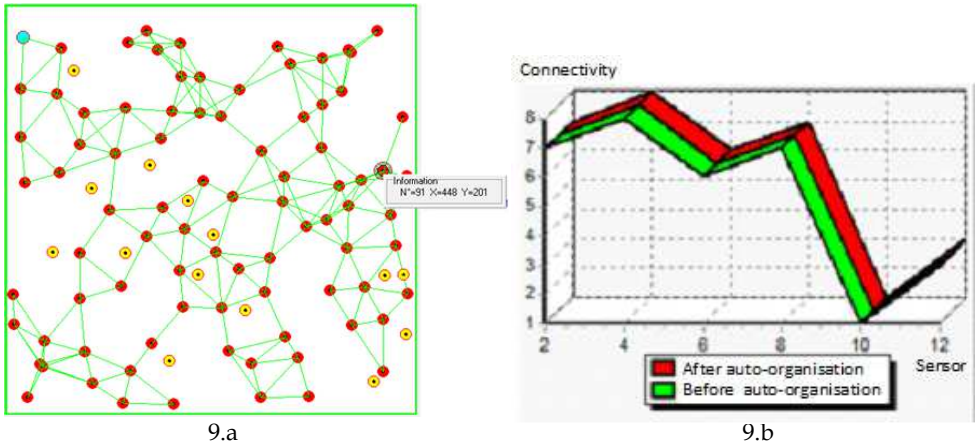
Fig. 7. Articulation point detection

After launch of self-organization algorithm, in first iteration some of articulation points are disparate by wake-up or move redundant nodes near articulation points. Following screenshot illustrate this.,



8.a 8.b

Fig. 8.a, 8.b. Self-organization after the first iteration.



9.a 9.b

Fig. 9.a, 9.b Self-organization after the last iteration

Per example: the node number 26 which was the articulation point has become a normal node after self-organization. The degree of connectivity around the point of articulation is increased, as shown in the figure 8; the green graph shows the connectivity before self-organization, the red graph shows the connectivity after self-organization. For next's iterations of self- organization we see the same for nodes number 9, 30, 31, 11 and 72. In the last iteration of self-organization, on notice that it remains one articulation point unresolved. As shown in figure 9, graphs of the degree of connectivity are the same.

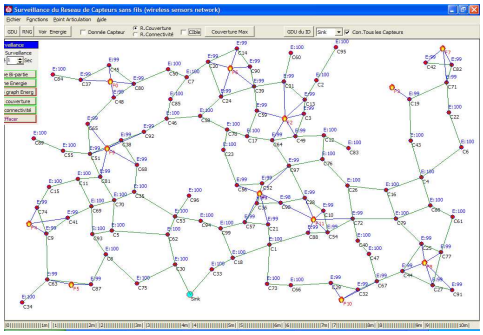


Fig. 10. Deployment and coverage targets

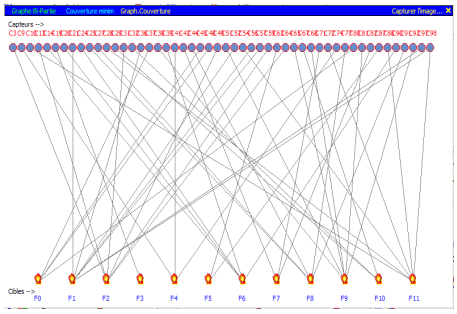


Fig. 11. Bipartite graph showing the maximum coverage of the various targets

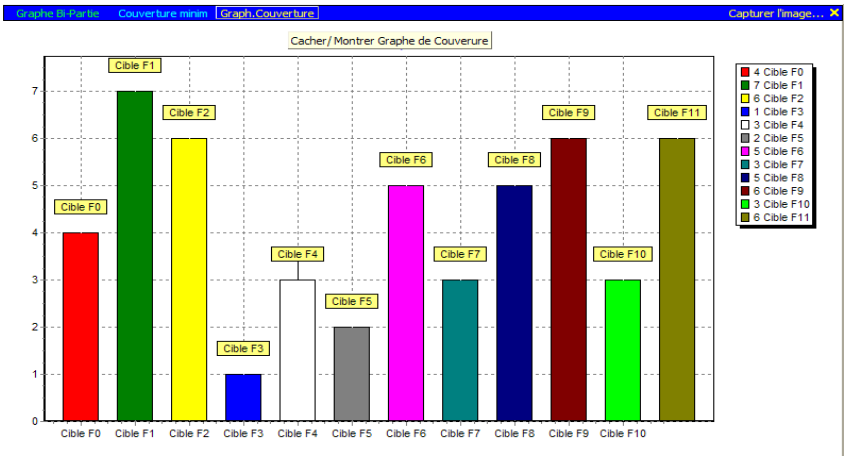


Fig. 12. Statistical state of the cover of each target

Figure 12 shows us results for the statistical state of target coverage. This highlights the heavily covered targets, indicating increased fault tolerant areas. Those that are poorly covered may require a reconfiguration or self-organization of the network.

4. Security in Wireless Sensor Networks Using Distributed Monitoring Mechanisms

4.1 Introduction

Wireless sensors networks are becoming increasingly interesting in recent years. These networks typically consist of hundreds or thousands of small sensors with limited resources (battery, bandwidth, processor, memory), to monitor some phenomena. The characteristics of such networks, such as fault tolerance, self-organization, the detection of high fidelity, low cost and rapid deployment have created many new applications of these networks, such as monitoring of wildlife, disaster response, military surveillance, industrial quality control and buildings intelligent, etc. [1]. However, the open nature of wireless communication, lack

of infrastructure deployment in hostile environments where they are highly exposed to physical vandalism and cooperation for the transmission of data, makes them very vulnerable to a wide type of attacks [53,54,55], including attacks against control traffic data as the Wormhole attack, the Rushing attack, the Sybil attack, Sinkhole attack, and the Hello flood attack.
An attack against data traffic includes Blackhole attack and the Selective forwarding attacks. Conventional techniques security, such as antivirus, IDS, encryption mechanisms, can not only prevent these attacks because many of them, such as Wormhole and rushing attacks can be launched without violating of any cryptographic mechanisms. To address these attacks, many researchers have used the concept of centralized monitoring, where a control center is responsible for monitoring all network nodes (such as base station, the central controller or manager, and sink) [56]. Other researchers have used a decentralized approach to monitor network nodes as fault detection through the coordination of neighboring [57,58,59]. The use of watchdog to detect misbehaviour neighbors [60], nodes guards are normal nodes in the network that perform basic operations such as the capture event, in addition to monitoring. Other research using the local monitoring between neighbouring nodes [61, 62]. In local monitoring, nodes monitor some traffic entering and leaving their neighbours for the detection of malicious behaviour.
From this work, nobody thought to use monitoring based on cluster architecture where each cluster member node performs a periodic calculation of certain metric necessary for making local decision at level cluster head. At each change of its state, member nodes sends its report to the cluster Head with a synchronization mechanism between nodes to minimize interference and reduce the number of packets delayed in transmission. Then a mechanism for optimizing the selection of a Cluster Head, who it is responsible for taken a local decision and monitoring the cluster members nodes. Finally, the base station aggregates the results received from different clusters Head and begins a global and centralized monitoring of network status, which can detect abnormalities that require global information network, reducing the flow of communication and the number false alarms. The main challenge of our works is to have a distributed monitoring for security reasons based on a clustered architecture, using a set of rules for diagnosing the status of sensors. The remainder of the sub chapter is organized as follows: Section 4.2 summarizes security in sensor networks, with detailed study of some attacks; the details of our approach are described in Section 4.3. In Section 4.4, we present our simulation results. Finally, we conclude this paper in Section 5.

4.2 Security in Wireless Sensor Networks

A. Attacks on sensor networks
For securing the Wireless Sensor Networks, it is necessary to address the attacks on WSN. This section lists and gives brief discussion about the major attacks against Wireless Sensor Network. Basically attacks are classified as active attacks and passive attacks [63,64,65,66,67,68,69]:

1) Passive Attacks
The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack, such as attacks against privacy.

2) Active Attacks

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active: Figure 1 shows the attacks classification on Wireless Sensor Networks.

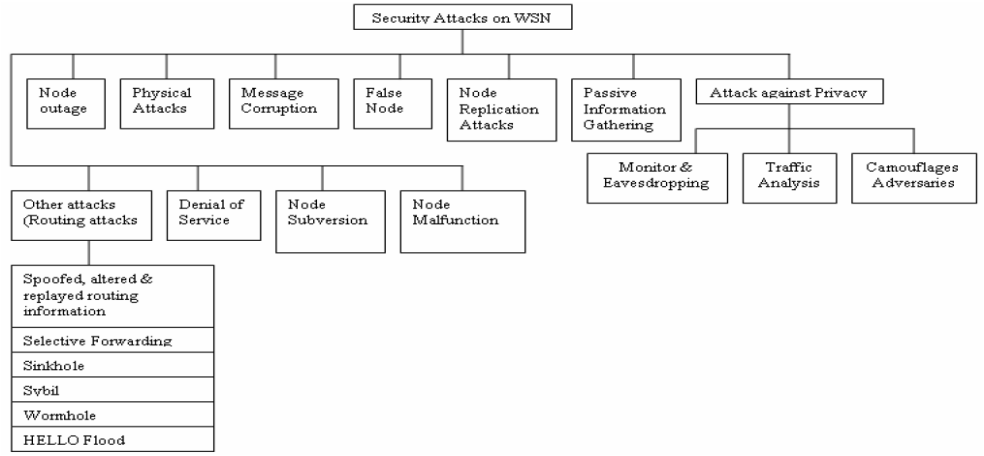


Fig. 1. Attacks classification on WSN.

B. Misbehavior in Wsn

Misbehavior in Wireless sensor network can be classified into two main categories, namely selfish nodes and malicious nodes [70]. These two types can cause real security threats in that they are the main reason for two of the main attacks that can damage MANET, and can be difficult to detect. Selfish node is the one behind the drop packets attack, where as malicious node is the one causing the denial of service (DoS) attack.

C. Anomaly Detection

Traditionally, intrusion detection techniques are classified into two broad categories: misuse detection and anomaly detection. Misuse detection works by searching for the traces or patterns of well-known attacks. Clearly, only known attacks that leave characteristic traces can be detected that way. Anomaly detection, on the other hand, uses a model of normal user or system behavior and flags significant deviations from this model as potentially malicious. This model of normal user or system behavior is commonly known as the user or system profile. A strength of anomaly detection is its ability to detect previously unknown attacks.

4.3. Our Approach

Network monitoring is an interesting approach that allows collecting the required information in order to analyze the behavior of the network. Monitoring in wireless sensor networks can be local with respect to a node or global with respect to the network. In sensor networks, local monitoring is not sufficient to detect some types of errors and security anomalies. For this reason we adopt in this paper a hybrid approach, the global monitoring approach based on a distributed monitoring. In general the existing failure detection approaches in WSNs is classified into two types: centralized and distributed approach. In

our case, the observers are the network nodes themselves. They perform a collaborative observation action. At first each node collects its security metrics (local traffic trace, resources consumption) and sends it to the local observer. We assume here that all the nodes have the collector and analyzer program running on their systems.

A. System Architecture

An example of our approach is illustrated in Figure 2. It consists of several coordinating components, namely: a large number of sensing nodes, several monitoring nodes, and base station.

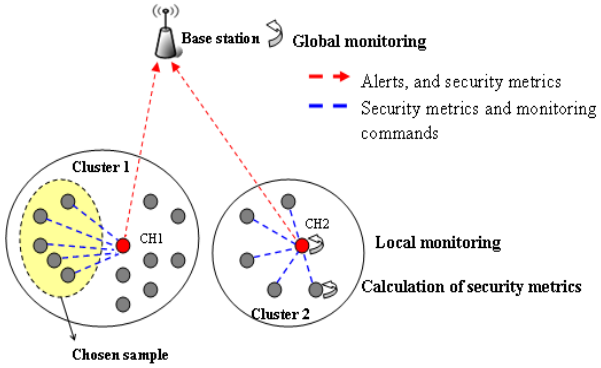


Fig. 2. Distributed Monitoring

Sensing nodes: Sensing nodes are small, resource constrained sensor nodes such as the Mica mote. They organize themselves into a network, sense and relay real-life measurements toward the networks.

Monitoring Nodes: Monitoring nodes have processing and communication capabilities. Each monitoring node covers a portion of the network topology (a cluster), where the sensor network will organize into a cluster formation, with each cluster head at a monitor.

Base Station: The main role of the base station is to make filtering and correlation of alerts and information sent by different monitors (the cluster-heads). Then thereafter it performs a more overall monitoring to detect hidden abnormalities that require an overview of information from the network. All these different entities are indispensable to our distributed Monitoring system. The system complexity and resource requirements increase progressively from sensing nodes, monitoring nodes, to base station.

B. Selection of a sample

The target population to be monitored is usually too large and for reasons of cost, and time, it is practically impossible to analyse all the member nodes in a population of a cluster. In general, we use the formula (3) for compute the number of nodes in the chosen sample [71]:

$$n = \frac{n_0}{1 + \frac{n_0}{N}} \tag{3}$$

Where :

- N is the size of population
- n is the size of chosen sample
- n0 a fixed value, n0 = 385

n = 385 / (1+385/N) to find the size needed (so the margin of error in estimating the proportion is less than 5% and, for a confidence level of 95%). The objective is to construct a sample so that observations can be generalized to the entire population. It is necessary that the sample has the same characteristics as the target population. In other words, it is representative. If this is not the case, the sample is biased.
The attribute state-sc(S_J), indicates the participation of sensor node S_J in the sample or not. For each sensor node $S_J \in$ cluster i, we have:

$$State - sc(S_J) = \begin{cases} 1 \ if \ S_J \ participate \ in \ the \ sample \\ 0 \ \ Otherwise \end{cases} \quad (4)$$

Example: if the number of member node N in the cluster i is 385, in this case the chosen sample n it equal to 192. For each period of monitoring the cluster- head can monitor 192 nodes.

C. Calculation of security metrics

This operation is done at each member node of a chosen sample in the cluster. The node performs after every epoch of time a calculation on its metrics of security, to assess their health status, such a level of energy consumption, level of memory usage, behavior of the nodes, etc. Figure 3 shows the process of metrics computing in member nodes. This node manages functions such as capturing, sending and receiving data messages, in addition to the functions of calculation of a security metrics like: the number of incoming and outgoing packet in a time interval, number of dropped packets, etc. Among the population of member nodes in the cluster, one representative sample of the population is chosen randomly. This sample will be analyzed in the period of ongoing monitoring. Each node in a chosen sample performs a calculation of his status. Once a difference in status between two time intervals is detected a calculated indicators values of security will be sent to the cluster Head for analyses.

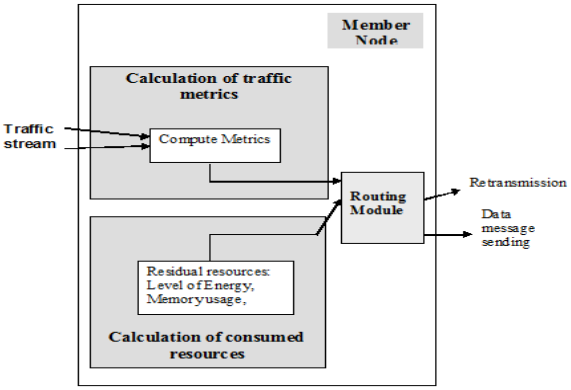


Fig. 3. Calculation of security metrics in each member node of a chosen sample

When sensor data are transmitted to the cluster head, nodes do not transmit sensor data if their data are not changed since last reported. For example, at the current round, sensor member S1 does not transmit its data to the cluster head because its data equal the collected data at the next round.

D. Local Monitoring in Cluster Head

The Cluster Head in figure 4, manages only the functions: self-monitoring of its state, local monitoring of the results obtained from the member nodes of its cluster, the reception and the emission of the messages, but does not manage, the function of capture of event. Cluster head is good at making decision because it has both network-level information and host-based information of all its nodes. The Cluster Head aggregates the results and send them to the base station for more global analysis; this strategy reduces the number of alerts gone up towards the base station.

- Cluster head can monitor its nodes thus to save their resources, or it can collect monitoring report from nodes and do some additional work.
- Cluster head is good at making decision because it has both network-level information and host-based information of all its nodes.

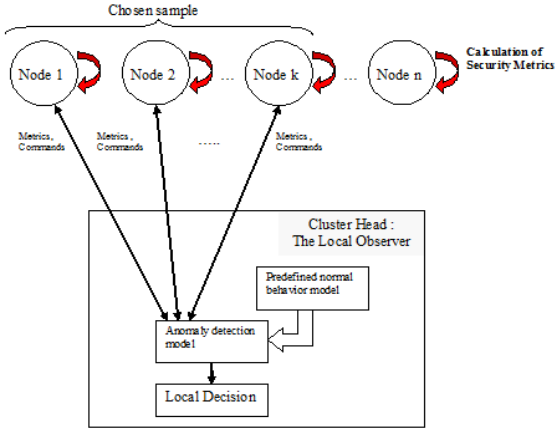


Fig. 4. Local Monitoring

E. Global Monitoring

The global observer receives the local traces collected by the local observers (the clusters-head) in order to analyze them. The first step toward performing this analysis is to correlate the traces and order them chronologically. In the network, all the nodes run with the same clock value allowing thus to perform the trace correlation.

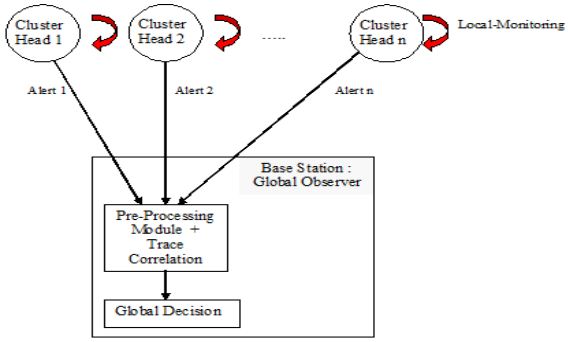


Fig. 5. Global Monitoring in Base Station

In First, the global observer collected alerts, have to be analyzed using a pre-processing module that performs the following tasks:

- Filtering the collected alerts keeping only the relevant information.
- Alert correlation and the construction of a unique global trace file.

F. Distributed Monitoring based clustering architecture

Clustering facilitates the distribution of control over the network. Clustering saves energy and reduces network contention by enabling locality of communication.

In our case, sensor networks are divided into cluster. The reorganization of the cluster will be made for a security reason, where each cluster Head monitors the member nodes of their cluster, which also facilitates the risen of alerts and reduces latency problems. These clusters are generated automatically after an epoch of clusters formation. Every cluster is assigned a cluster head CH, by election with some metrics. We opted for an election of cluster head according a new metrics based on multiple criteria decision approach to decision support for the selection of CHs, the criteria are: the criterion of density (the degree of connectivity of each node), the criterion of energy (the level of residual energy in each node), the distance between nodes in the cluster, the behavior level of each node and the index of mobility. Each node calculates its metrics locally, then evaluates a function of weight according to these metric (each node is limited to the closest neighbors), and diffuses the value of this function to its neighbors. Cluster Head of each cluster is then elected of these results. Three constraints which are the fact, that two CH cannot be coast at coast, and that if a node belongs to two clusters, it must belong with the nearest cluster (by using a parameter of distances), finally if a node is completely isolated it becomes automatically a cluster Head.

1) Clustering algorithm metric

We describe in this section, the metric used in our algorithm for clustering formation, then we present its election protocol and update policy. The updating policy is locally called after mobility or -adding new nodes in the network. To decide how much a node is suited for being a cluster head to offer security services, we take into consideration the following characteristics:

The node behaviour level B(i,t): Nodes with a behaviour level less than a threshold behaviour-Min will not be accepted as candidate for being cluster heads even if they have other interesting characteristics as high energy, high degree of connectivity or low mobility. First of all each nodes are assigned a same static behaviour level B=1. However, this level can be decreased by the anomaly detection algorithm if a nodes are misbehaving B=B – rate. Classification of the behaviour value takes the following values:

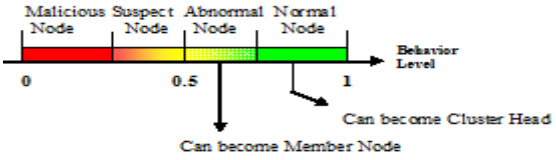


Fig. 6. Behavior Level, B∈[0,1]

Classification of the behaviour value takes the following values:

$$\begin{cases} Normal\ Node: 0.8 \le B \le 1 \\ Abnormal\ Node\ (\text{but not malicious}): 0.5 \le B < 0.8 \\ Suspect\ Node: 0.3 \le B < 0.5 \\ Malicious\ Node: 0 \le B < 0.3 \end{cases} \quad (5)$$

The node mobility M(i,t): We aim to have stable clusters. So, we should elect nodes with low relative mobility as cluster heads. To characterize the instantaneous nodal mobility, we will use a simple heuristic mechanism [71,72] where each node i estimates its relative mobility index Mi by implementing the following procedure:
Compute the running average of the speed for every node i till current time T. This gives a measure of mobility and is denoted by M_i , as:

$$M_i = \frac{1}{T} \sum_{t=1}^{T} \sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2} \quad (6)$$

Where (x_t, y_t) and (x_{t-1}, y_{t-1}) are the coordinates of the node v at time t and (t -1) , respectively.

The distance to neighbors D(i,t): It is better to elect the node with the nearest members as a cluster head [73,74].
For every node i, compute the sum of the distances, D_i, with all its neighbors j , as :

$$D_i = \sum_{j \in N(i)} \{dist\ (i, j)\} \quad (7)$$

The node remaining energy E(i,t): We should elect nodes with high remaining battery power as cluster heads. The radio spends $E_{Tx\text{-}elec} = E_{Rx\text{-}elec} = E_{elec}$ energy to run receiver and transmitter electronics. Therefore the transmission cost to transfer k-bit message to a distance d is given by the equation (8) [75]:

$$E_{Tx}(k,d) = \{kE_{elec} + kE_{amp}d^2 \quad (8)$$

Where E_{amp} is a required amplifier energy. Similarly, the receiving cost can be given by equation (9) :

$$E_{Rx\ elec}(k) = kE \quad (9)$$

The node connectivity degree C(i,t):
N(i) is the neighbors of node i , defined as [52] :

$$N[i] = \bigcup_{j \in V,\ j \ne i} \{ j \mid dist\ (i, j) < tx_{range} \} \quad (10)$$

Find the neighbors of each node i which defines its degree d_i as :

$$C_i = |N(i)| = \left| \sum_{j \in V, j \neq i} \{ dist(i, j) < tx_{range} \} \right| \quad (11)$$

We should elect nodes with very high connectivity as cluster heads.
Each node S_i computes its **weight P_i** according to the method of weighted sum decision model, given by equation (12) :

$$P_i = w_1 * B_i + w_2 * Er_i + w_3 * M_i + w_4 * C_i + w_5 * D_i \quad (12)$$

where w_1, w_2, w_3,w_4,w_5 are the weighing factors for the corresponding system parameters, such that ($w_1+w_2+w_3+w_4+w_5=10$), and since our goal is to monitor sensor we taken a high coefficients for the behavior B_i and the remaining energy Er_i, as follows: $w_1=4$, $w_2=3$, $w_3=1$, $w_4=1$, $w_5=1$.

2) Node Status

A node in wireless sensor network can be in one of the 3 possible states: MEMBER (ME), HEAD (CH), Monitor Node or Guard node (MO). Initially, every node is in ME state. It starts election and may become CH node if it does not have link to any CH node, otherwise it still a member ME.

3) Proposed Methodology

Our goal is to detect malicious activities in the network caused by the attacks and the failure of nodes. We will offer primarily an organization of cluster network, where the cluster- head of each cluster is responsible for monitoring the member nodes of its cluster. Subsequently we propose a system for detecting anomalies based on a distributed approach.

4.4 Simulation and Results

In this section, we present the simulation model and results of our work.

4.4.1 Simulation model

We developed a wireless sensor network simulator to create an environment to evaluate our work. It is a discrete event simulator written in C++. A network generator was built, which generates networks comprised of normal nodes plus malicious node, all located in an square field. Each node has randomized x and y coordinates. No two different nodes share the same coordinates. In our simulation, the sensor nodes are randomly distributed in a 880mx360m square field, the communication range is 150m. The scenario simulation consists of two steps: the first is for the formation of cluster, the second is to monitor the network by different cluster head and the detection of the abnormal behaviour. For the simulation of abnormal behaviour in the network, we generated a number of malicious nodes that their state will move from a normal node with green colour to a abnormal node with yellow colour, to a suspicious node of red colour , and lastly, a malicious node with black colour. All the states of member nodes are detected by their cluster head. Malicious cluster head are detected by the base station.

4.4.2 Results

In the following, we present and discuss the simulation results.

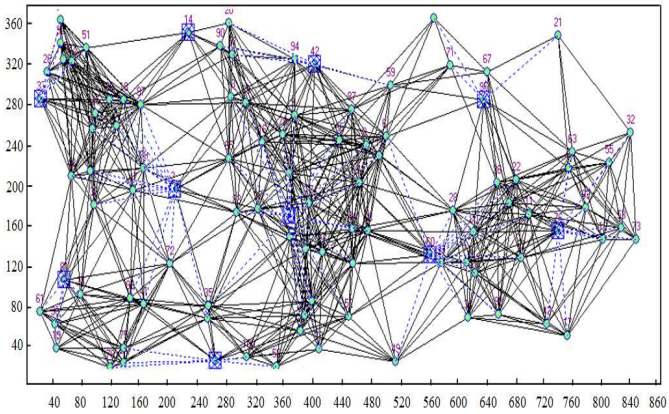


Fig. 7. Random deployment and graph connectivity of 100 nodes in square field.

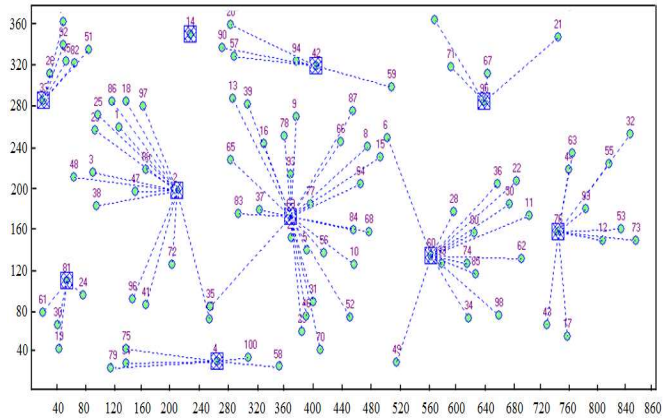


Fig. 8. Network after Clustering Formation

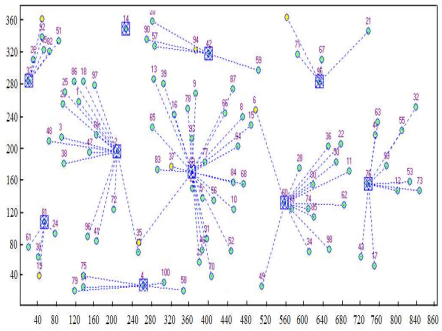


Fig. 9. Sensors with yellow colour are abnormal but not malicious

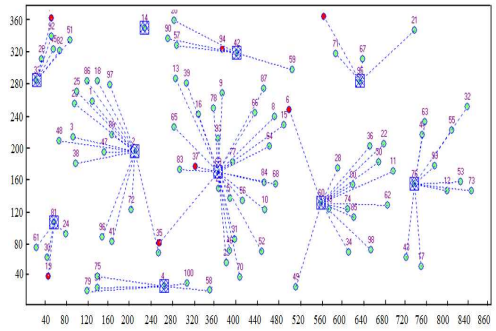


Fig. 10. the red sensors have a suspect behaviour

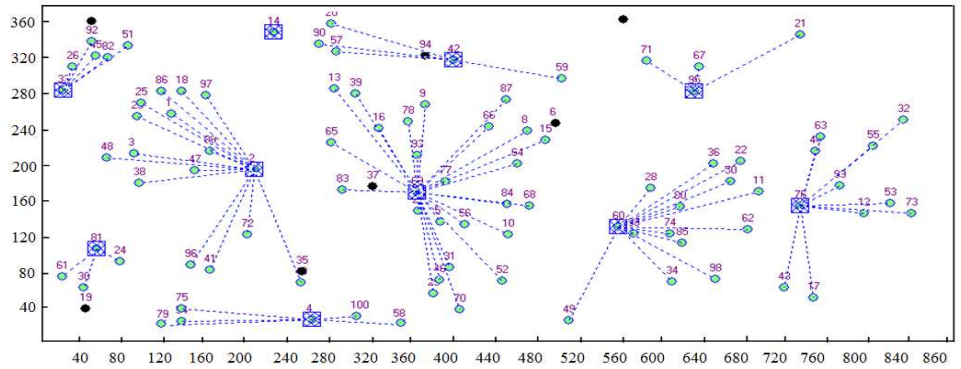


Fig. 11. The sensors with black color are compromised and have an malicious behavior

The black sensors will be placed in a black list and will be disconnected from the network, as shown in Figure 11.

5. Conclusion

In this chapter we started with the presentation of the overview of the mechanisms of monitoring a wireless sensor networks, for the following reasons: topology control (connectivity and the coverage), and the security in wireless sensor networks. Then we have developed a new monitoring mechanism to guarantee strong connectivity in wireless sensors networks, this mechanism is based on the distributed algorithms. The mechanism monitors sensor connectivity and at any time is able to detect the critical nodes that represent articulation points. Such articulation points are liable to cause portions of the network to become disconnected and we have therefore also developed a mechanism for self-organization to increase the degree of connectivity in their vicinity, by increasing fault tolerance. Since connectivity is closely related to the coverage of targets, we have also developed a way to monitor the robustness of the coverage between fixed targets and sensor nodes. The main advantage of our approach is the ability to anticipate disconnections before they occur. We are also able to reduce the number of monitoring node and assume mechanisms for fault tolerance by auto organization of nodes to increase connectivity. Finally, we have demonstrated the effectiveness of our approach and algorithms with satisfactory results obtained through simulation.

After that we have presented our second contribution for the security of a wireless sensor networks based on the distributed monitoring mechanisms. We have presented a decentralized approach to monitor the status and behavior in a wireless sensor network. For this we have developed a completed distributed monitoring mechanism for securing wireless sensor networks. Based on a flexible weight clustering algorithm, a number of parameters of nodes were taken into consideration for assigning weight to a node and election cluster-head. The proposed algorithm chooses the robust cluster-heads who is the responsibility to monitor a chosen sample of nodes in their cluster, and maintains clusters locally. A second algorithm analyzes and detects a specific misbehavior in wireless sensor networks. This algorithm insures the update of a behavior-level metric and isolates the

misbehaving node. The advantage of our approach is the minimization of the communication between the monitor's nodes and the normal nodes.

6. References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cyirci, "Wireless Sensor Networks: A Survey.", Computer Networks, vol. 38, no.4, pp. 393-422, 2002.

[2] L. Kleinrock and J. Silvester. "Optimum transmission radio for packet radio networks or why six is a magic number. In National Telecommunications Conference, Birmingham, Alabama, pages 4.3.2–4.3.5, December 1978.

[3] A. Cerpa and D. Estrin, "Ascent: Adaptive self-configuring sensor networks topologies" IEEE Transactions on Mobile Computing, vol. 3, no. 3, pp. 272–285, 2004.

[4] N. Li and J. C. Hou, "Improving connectivity of wireless ad hoc networks", in MOBIQUITOUS '05: Proceedings of the The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services. Washington, DC, USA: IEEE Computer Society, 2005, pp. 314–324.

[5] M. Dunbabin, P. Corke, I. Vasilescu, and D. Rus, "Data muling over underwater wireless sensor networks using an autonomous underwater vehicle.", in IEEE International Conference on Robotics and Automation (ICRA), 2006, May 15- 19 2006, pp. 2091–2098.

[6] K. Benahmed, H. Haffaf , M. Merabti, D. Llewellyn-Jones, "Monitoring Connectivity in Wireless Sensor Networks ", International Journal of Future Generation Communication and Networking, Vol. 2, No. 2, 2009.

[7] G. Yang, L.-J. Chen, T. Sun, B. Zhou, and M. Gerla, "Ad-hoc storage overlay system (asos): A delay-tolerant approach in manets.", in Proceeding of the IEEE MASS, 2006, pp. 296–305.

[8] N. Rao, W. Qishi, S. Iyengar, and A. Manickam, "Connectivity-through-time protocols for dynamic wireless networks to support mobile robot teams.", in IEEE International Conference on Robotics and Automation (ICRA), 2003, vol. 2, Sept 14-19 2003, pp. 1653–1658.

[9] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin Highly-Resilient, "Energy-Efficient Multipath Routing in Wireless Sensor Networks.", Mobile Computing and Communications Review, 1(2), 1997.

[10] D. Spanos and R. Murray, "Motion planning with wireless network constraints.", in Proceedings of the 2005 American Control Conference, 2005, pp. 87–92.

[11] D. Desovski, Y. Liu, and B. Cukic. "Linear randomized voting algorithm for fault tolerant sensor fusion and the corresponding reliability model.", In IEEE International Symposium on Systems Engineering, pages 153–162, October 2005.

[12] A. Boukerche, "Handbook of Algorithms and Protocols for Wireless and Mobile Networks", Chapman CRC/Hall, 2005.

[13] N. Li and J. C. Hou. "FLSS: A Fault-Tolerant Topology Control Algorithm for Wireless Networks.", In Proceedings of the 10th Annual International Conference on Mobile Computing and Networking, pages 275–286, 2004.

[14] J. L. Bredin, E. D. Demaine, M. Hajiaghayi, and D. Rus. "Deploying Sensor Networks with Guaranteed Capacity and Fault Tolerance.", In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pages 309–319, 2005.

[15] Bahramgiri, M., Hajiaghayi, M., and Mirrokni, "Fault-tolerant and 3-dimensional distributed topology control algorithms in wireless multi-hop networks.", 2002.

[16] N. Li, J. Hou, and L. Sha. "Design and analysis of an mst-based topology control algorithm." , In Proceedings of the IEEE INFOCOM, 2003.

[17] Xiang-Yang Li, Peng-Jun Wan, Yu Wang, and Chih-Wei Yi. "Fault tolerant deployment and topology control in wireless networks.", In Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing (MobiHoc), pages 117.128, 2003.

[18] Michaël Hauspie , "Contributions à l'étude des gestionnaires de services distribués dans les réseaux ad hoc ", Thèse de doctorat, Université des Sciences et Technologies de Lille, 2005.

[19] Bruno Courcelle, " Introduction à la théorie des graphes: Définitions, applications et techniques de preuves ", Université Bordeaux 1, LaBRI (CNRS UMR 5800), 20 Avril, 2004.

[20] R. Tarjan., "Depth First Search and linear graph algorithms.", SIAM Journal of Computing, 1:146_160, 1972.

[21] Wies law Zielonka , "Algorithmique ", LIAFA, Université Denis Diderot, Septembre 2006.

[22] K. Chakrabarty, S. S. Iyengar, H. Qi, E. Cho, "Grid coverage for surveillance and target location in distributed sensor networks," IEEE Transactions on Computers, 51(12):1448-1453, December 2002.

[23]S. Meguerdichian and M. Potkonjak. "Low Power 0/1 Coverage and Scheduling Techniques in Sensor Networks." UCLA Technical Reports 030001. January 2003.

[24]S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. Srivastava, "Coverage Problems in Wireless Ad-Hoc Sensor Networks." IEEE Infocom 2001, Vol 3, pp. 1380-1387, April 2001.

[25] S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak, "Exposure in Wireless Ad Hoc Sensor Networks." Procs. of 7th Annual International Conference on Mobile Computing and Networking (MobiCom'01), pp. 139-150, July 2001.

[26] T. Couqueur, V. Phipatanasuphorn, P. Ramanathan and K. K. Saluja, "Sensor Deployment Strategy for Target Detection," Proceeding of The First ACM International Workshop on Wireless Sensor Networks and Applications, Sep. 2002.

[27] D. Tian and N.D. Georganas, "A Coverage-preserved Node Scheduling scheme for Large Wireless Sensor Networks," Proceedings of First International Workshop on Wireless Sensor Networks and Applications (WSNA'02), Atlanta, USA, September 2002.

[28] A. Cerpa and D. Estrin, "ASCENT: Adaptive Self-Configuring Sensor Networks Topologies," International Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2002), New York, NY, USA, June 23-27 2002.

[29] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks," ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2001), Rome, Italy, July 16-21, 2001.

[30] Y. Xu, J. Heidemann, and D. Estrin, "Adaptive Energy-Conserving Routing for Multihop Ad Hoc Networks," Research Report 527, USC/Information Sciences Institute, October 2000.

[31] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed Energy Conservation for Ad Hoc Routing," ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2001), Rome, Italy, July 16-21, 2001.

[32] F. Ye, G. Zhong, S. Lu, and L. Zhang, "PEAS: A Robust Energy Conserving Protocol for Long-lived Sensor Networks". The 23rd International Conference on Distributed Computing Systems (ICDCS'03), May 2003.

[33] A. Perrig, "SPINS: security protocols for sensor networks," In Proc. of ACM MobiCom, 2001.

[34] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," In Proc. Of ACM SASN, 2004.

[35] I. Khalil, S. Bagchi, and C. Nina-Rotaru, "DICAS: detection, diagnosis and isolation of control attacks in sensor networks," In Proc. of IEEE SecureComm, 2005.

[36] S.-B. Lee and Y.-H. Choi, "A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks," In Proc. of ACM SASN, 2006.

[37] I. Khalil, S. Bagchi, and N. Shroff, "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks," In Proc. of IEEE/IFIP DSN, 2005.

[38] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," In Proc. Of ACM SASN, 2004.

[39] [S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol: cooperation of nodes fairness in distributed ad-hoc networks," In Proc. of ACM MobiHoc, 2002.

[40] P. Michiardi and R. Molva, "CORE: a collaborativereputation mechanism to enforce node cooperation in mobile ad hoc networks," In Proc. of the IFIP Sixth Joint Working Conference on Communications and Multimedia Security, 2002

[41] K. Ioannis, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," In Proc. of the 13th European Wireless Conference, 2007.

[42] Y. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," In Proc. of ACM SASN, 2003.

[43] I. Khalil, S. Bagchi, and N. B. Shroff, "SLAM: sleep-wake aware local monitoring in sensor networks," In Proc. Of IEEE/IFIP DSN, 2007.

[44] C. Hsin and M. Liu, "Self-monitoring of wireless sensor networks," Elsevier Computer Communications, vol. 29, pp.462-476, 2006.

[45] T. H. Hai1, E.-N. Huh, and M. Jo,"A lightweight intrusion detection framework for wireless sensor networks", Wirel. Commun. Mob. Comput. (2009)

[46] Q. Wang, T. Zhang , "Detecting Anomaly Node Behavior in Wireless Sensor Networks", 21st International Conference on Advanced Information Networking and Applications Workshops, 2007.

[47] K. Ramachandran, E. M. Belding-Royer, and K. C. Almeroth. DAMON: A Distributed Architecture for Monitoring Multi-hop Mobile Networks. In Proceedings of the 1st IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON), October 2004.

[48] J. Zhao, R. Govindan, and D. Estrin. Residual energy scans for monitoring wireless sensor networks. In IEEE Wireless Communications and Networking Conference (WCNC), 2002.

[49] NIthya Ramanathan, Kevin Chang, Rahul Kapur, Lewis Girod, Eddie Kohler, Deborah Estrin. Sympathy for the Sensor Network Debugger. In 3rd Embedded networked sensor systems. 2005. San Diego, USA: ACM Press.

[50] Y. an Huang and W. Lee, A cooperative intrusion detection system for ad hoc networks, in Proc of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, 2003, pp. 135–147.

[51] S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in Mobile Computing and Networking, 2000, pp. 255–265.

[52] K. Benahmed, H. Haffaf, M. Merabti, D. Llewellyn-Jones, "Monitoring connectivity in Wireless Sensor Networks", IEEE Symposium on Computers and Communications (ISCC'09), Sousse, Tunisia, 5-8 July 2009.

[53] Tanya Roosta, Shiuhpyng Winston Shieh, S. Shankar Sastry. "Taxonomy of Security Attacks in Sensor Networks and Countermeasures ". The First IEEE International Conference on System Integration and Reliability Improvements, December, 2006.

[54] T.Kavitha, D.Sridharan, "Security Vulnerabilities In Wireless Sensor Networks: A Survey", Journal of Information Assurance and Security 5 (2010) 031-044

[55] Song Han, Elizabeth Chang, Li Gao and Tharam Dillon, "Taxonomy of Attacks on Wireless Sensor Networks", Proceedings of the First European Conference on Computer Network Defence School of Computing, University of Glamorgan, Wales, UK, 2005.

[56] M.Yu, H.Mokhtar, M.Merabti,"A Survey on Fault Management in Wireless Sensor Networks", School of Computing & Mathematical Science Liverpool John Moores University. UK, 2007.

[57] Chihfan Hsin, Mingyan Liu. A Distributed Monitoring Mechanism for Wireless Sensor Networks. in 3rd workshopo on Wireless Security. 2002: ACM Press.

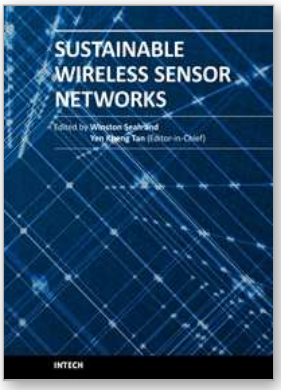
[58] Jinran Chen, Shubha Kher, Arun Somani. Distributed Fault Detection of Wireless Sensor Networks. in DIWANS'06. 2006. Los Angeles, USA: ACM Pres.

[59] Anmol Sheth, Carl Hartung, Richard Han. A Decentralized Fault Diagnosis System for Wireless Sensor Networks. in 2nd Mobile Ad Hoc and Sensor Systems. 2005. Washington, USA.

[60] Sergio Marti, T.J.Giuli, Kevin Lai, Mary Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. in 6th International Conference on Mobile Computing and Networking. 2000. Boston, Massachusetts, USA: ACM.

[61] Y. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 135-147, 2003.

[62] A. Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, pp. 16-23, 2005.
[63] M. Saraogi, "security in wireless sensor networks" , University of Tennessee, 2005.
[64] J.P. Mäkelä, "Security in Wireless Sensor Networks", Oulu University of Applied Sciences, School of Engineering, Oulu, Finland, 2009.
[65] J. Rehana, "Security of Wireless Sensor Network" Helsinki University of Technology, Helsinki, Technical Report TKK-CSE-B5, 2009.
[66] I. Chatzigiannakis, "A Decentralized Intrusion Detection System for Increasing Security of Wireless Sensor Networks", University of Patras, Greece, 2007.
[67] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures". In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (Anchorage, AK, May 11, 2003).
[68] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Proceedings of 8th IEEE ICACT 2006, Volume II, February 20-22, Phoenix Park, Korea, 2006, pp. 1043-1048.
[69] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary ,"Wireless Sensor Network Security: A Survey", in Distributed, Grid, and Pervasive Computing, Yang Xiao (Eds.), 2006.
[70] E. Z. Ang, "Node Misbehaviour in Mobile Ad Hoc Networks," National University of Singapore, 2004.
[71] A. H. Hussein, A. O. Abu Salem, S. Yousef ,"A Flexible Weighted Clustering Algorithm Based on Battery Power for Mobile Ad Hoc Networks", IEEE, 2008.
[72] C. Li, Y Wang, F. Huang, D. Yang," A Novel Enhanced Weighted Clustering Algorithm for Mobile Networks", IEEE 2009.
[73] B. Kadri, A. M'hamed, M. Feham , "Secured Clustering Algorithm for Mobile Ad Hoc Networks", IJCSNS , VOL.7 No.3, March 2007.
[74] M. Chatterjee, S. K. DAS, D. Turgut, "WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks", Cluster Computing 5, 193–204, 2002.
[75] Z. J.-wu, J. Y.-ying, Z. J.-ji, Y. C.-lei,"A Weighted Clustering Algorithm Based Routing Protocol in Wireless Sensor Networks ", ISECS 2008.



Sustainable Wireless Sensor Networks

Edited by Yen Kheng Tan

ISBN 978-953-307-297-5
Hard cover, 574 pages
Publisher InTech
Published online 14, December, 2010
Published in print edition December, 2010

Wireless Sensor Networks came into prominence around the start of this millennium motivated by the omnipresent scenario of small-sized sensors with limited power deployed in large numbers over an area to monitor different phenomenon. The sole motivation of a large portion of research efforts has been to maximize the lifetime of the network, where network lifetime is typically measured from the instant of deployment to the point when one of the nodes has expended its limited power source and becomes in-operational â€“ commonly referred as first node failure. Over the years, research has increasingly adopted ideas from wireless communications as well as embedded systems development in order to move this technology closer to realistic deployment scenarios. In such a rich research area as wireless sensor networks, it is difficult if not impossible to provide a comprehensive coverage of all relevant aspects. In this book, we hope to give the reader with a snapshot of some aspects of wireless sensor networks research that provides both a high level overview as well as detailed discussion on specific areas.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Khelifa Benahmed, Haffaf Hafid and Madjid Merabti (2010). Monitoring of Wireless Sensor Networks, Sustainable Wireless Sensor Networks, Yen Kheng Tan (Ed.), ISBN: 978-953-307-297-5, InTech, Available from: http://www.intechopen.com/books/sustainable-wireless-sensor-networks/monitoring-of-wireless-sensor-networks

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821