# Reasoning Services for Security and Energy Management in Wireless Sensor Networks

Maïssa Mbaye*, Hicham Khalife† and Francine Krief†
*LANI, Université Gaston Berger de St-Louis - Sénégal
Email: maissa.mbaye@ugb.edu.sn
†LaBRI, Université de Bordeaux France
Email: {name.surname}@labri.fr

***Abstract*—In this paper we propose a management scheme based on automated reasoning for wireless sensor networks. Our scheme ensures reliable zone surveillance with reduced energy consumption, a crucial constraint in sensors networks and in tomorrow's green communication platforms. We divide the zone to monitor into a set of areas each containing a management node that implements reasoning services. The management node centralizes alerts issued by sensors in the area, correlates them, and raises an alarm to the administrator only if a real event occurs. Moreover, each sensor runs a set of reasoning functions that limit its communication with the management node of its area. Through simulations we show that our scheme reduces considerably the number of messages sent from sensor to management nodes as well as alarms raised by the management nodes to the administrator without missing events in the monitored zone. Hence our management ensures reliable surveillance and extends the sensor network lifetime in the same time.**

## I. Introduction

Wireless Sensor Networks (WSN) reached a while ago the deployment phase offering today a set of services for diverse applications. Because they give the possibility of controlling diverse areas and track different set of environment parameters (temperature, humidity, etc), area monitoring and surveillance have attracted particular efforts from research and industry. Consequently, we observed in the last few years many WSN deployments targeting indoor and outdoor area monitoring, where new protocols at different layers of the protocol stack have been proposed. Essentially, many of these protocols consider optimizing energy consumption and channel contention as their primary objectives.

Today the maintenance costs and the limited lifespan of wireless sensor networks constitute an important disadvantage in their use. Therefore, developing autonomic WSN systems that can manage themselves so as to improve their efficiency and functionalities without the need for human intervention emerges as necessary solution to extend the network lifetime. In the vast majority of the previous initiatives, intelligence was not considered as an inherent functionality embedded in the WSN. Indeed, the main objectives were to propose techniques that increase the lifetime of the network [1], convey efficiently the information to the designated sinks [2], and to monitor the access and limit the losses on the wireless medium [3]. We argue that network efficiency and lifetime can be further increased if intelligent management is added in the network thus understanding the environment and taking measures accordingly. Clearly in order expand the sensor network lifespan, reducing the number of exchanged messages is a key factor that an intelligent management scheme needs to handle. Some undergone measurements show that the energy cost of 1 byte transmission can be more than 1000 times higher than executing an instruction. Moreover transmission/reception consumes energy at both the sender and the receiver, while computation tasks implicate a single sensor node. Hence, one can easily conclude that adding more computation (intelligence) and reducing the number of exchanged messages reduces the energy consumption in wireless sensor networks.

This work was supported by the French National Research Agency (ANR) under grant reference ANR-08-VERS-018.

In this paper, we propose a management scheme for wireless sensor networks based on reasoning services. A set of management functions are implemented such as environment discovery and detection of events in a monitored area with the objective limiting energy consumption. We define for each monitored area a criticality level and use specific reasoning tools to manage intrusion and security. In fact within each area, dependency between sensors and between different events is built based on Bayesian reasoning. Then, received alerts within each area are combined and normalized using intelligent techniques in order to raise alarms to the network administrator only if the criticality level Threshold of the area is attained or exceeded.

Through simulations, we validate the effectiveness of our solution. We show that our management scheme reduces considerably the number of sent messages in the sensor network. Indeed, by implementing reasoning services in each node of the network and adding a central management entity in each area, we empower sensors to manage intelligently and distributedly their environment variations. Furthermore, our solution reduces false positives by limiting alarms sent to administrator thus lowers the energy consumption due to communications. Few researchers have already used reasoning in sensor networks [4] [5], however the innovation in our management scheme resides in its capability to monitor and combine different types of received alerts coming from heterogeneous sensors.

## II. Considered Environment and Objectives

We consider a zone monitoring scenario where sensitive areas are manually identified. In each of these areas a number of sensor nodes are deployed randomly in a way to create redundancy. The nodes are of different types, for instance pressure nodes, temperature and humidity sensors can be deployed. All areas are in the communication range (directly or through multi-hop communication) of a control center where a human administrator is available. Note that a single control center exists in our architecture to which all areas are connected. This can be seen in Figure 1 .

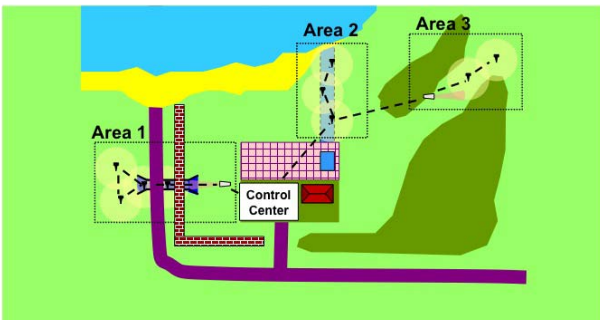


Fig. 1. A typical area monitoring scenario

We assume also that in each defined area, a node is elected as a management node (also called reasoning nodes). The details of the election mechanism can be based on energy, location and other constraints but are beyond the scope of this paper. The management node centralizes alerts received from all the sensors in the area and is the only node eligible to raise alarms to the control center.

### A. Management Objectives

Our goal is to ensure a reliable area monitoring with the major concern of reducing the power consumption of the wireless network. To achieve our objective we propose a management scheme for WSN based on automated reasoning services. Our scheme must ensure the following two objectives:

- Detect all intrusions in the system without missing any important event.
- Reduce energy consumption by limiting the number of alerts between sensors and management nodes of their areas and alarms between management nodes and control center. Practically, this can be seen as reducing false positives alarms as well as redundant alerts/alarms.

Clearly these two objectives are contradictory. Indeed, the challenge of our management platform is to reduce the number of sent messages while being sure of capturing all important events in the network. We overcome both challenges through the use of reasoning services.

## III. Reasoning for Management and Control

Because communication (i.e. sending and receiving messages) is the highest source of consumption in wireless devices, our architecture by using reasoning tools, reduces the number of exchanged messages between sensor and management nodes as well as alarms between management nodes and the control center. Moreover, the whole communication architecture in our WSN was conceived to be energy efficient. However we do not present in this paper the lower layers in order to focus on our management schemes based on the reasoning services. Note that throughout the paper we refer to alert as the message sent from a sensor to a management node whereas an alarm denotes the message destined to the control center.

### A. General Overview

The reasoning services operate on top of our communication architecture and exploit its capability to convey efficiently required information. We implement in our management scheme two variants of reasoning functions. In fact at every sensor level, intelligent functions are introduced to control the alerts sent to the reasoning nodes and their frequency. At the management node level, more advanced reasoning functions are deployed. The latter functions correlate dependant alerts and raise alarms to the administrator only if the criticality level threshold is exceeded.

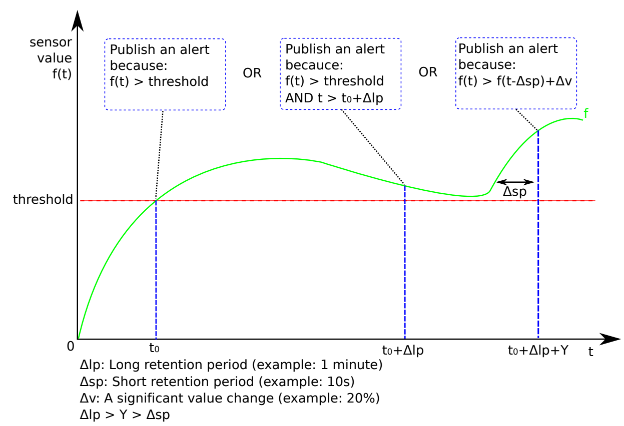


Fig. 2. Alerts by sensor nodes

More precisely at each sensor node in every monitored area, updates are sent to the management node. In order to lower energy consumption, alerts should be sent only when a significant variation in the sensed environment occurs. A sensor node should publish an alert that will be conveyed through our communication architecture to the reasoning node in the following two cases (cases are highlighted in Figure 2):

- When the sensed value becomes higher than a fixed threshold. This threshold represents the smallest value that could characterize an event/intrusion. This alert is sent to the reasoning node only if no previous alert was sent in the $\Delta_{lp}$ duration. Practically, this condition eliminates the scenario where the same event generates multiple alerts thus causing valuable energy waste.
- When the sensed value rises quickly (more than $\Delta_v$ units in less than $\Delta_{sp}$ duration). Before sending this alert, sensors verify that no message to the reasoning node was

sent in the last short period duration (denoted by $\Delta_{sp}$ in the Figure). This case allows the reasoning services to capture a quick variation in the environment even if an alert was already sent since a period shorter than the long period duration $\Delta_{lp}$.

### B. Criticality Level

In the management node, the reasoning services role is to gather data from surrounding sensors then combine the dependant sensor values in order to trigger alarms. Raised alarms are then conveyed through our communication architecture to the administrator in charge of the security of the area. As in all artificial intelligence related areas, reasoning tools require a learning phase [6]. In our particular case, in every monitored area dependency between occurring events should be computed. We use a Bayesian reasoning (conditional relationships) to compute the degree of relation between observed phenomena in each area. This can be done by using Bayes theorem for the conditional probability $P(A|B) = \frac{P(A \cap B)}{P(B)}$. For instance, the management node in every area, computes the dependency between events $A$ and $B$ by counting during the training phase the number of times these two events occur simultaneously. Note that within each area, some events might not be correlated while others coming from different types of sensors can be highly dependant.

After learning the dependency between the sensors of each area, the management node becomes ready for receiving alerts, combining them, then raising alarms if necessary. More precisely, the alarm is raised if reasoning node finds that a criticality level threshold (defined hereafter) is exceeded. The decision process that the reasoning service runs is based on the value of all the sensors of the monitored area. In fact, when a sensor value goes higher than a threshold, a message is sent to the area reasoning node. This alert raises the criticality level of the area by a number that depends on the sensor type and the reputation of the sensor. The criticality will then decrease linearly as time passes unless another *dependant* sensor in the same area detects an event and sends an alert to the reasoning node. If cumulating alerts of correlated sensors within the area makes the criticality level goes higher than a threshold, then the management node raises an alarm to the network administrator. A visual example is given in Figure 3. The criticality level objective is twofold. First it offers a tool to manage the importance and the relevance of alerts within an area. Indeed, cumulating related alerts before sending an alarm to the control center reduces false alarms as well as energy consumption thus extends the network lifetime. Second, it allows us to combine different types of alerts coming from different types of sensors. This can be done by normalizing alerts through multiplying them by a factor depending on their type (i.e temperature, humidity, and pressure).

Besides, the criticality level can also help the management node to assign a weight for each alert based on the confidence it has in issuing sensor. In fact, reasoning functions can include reputation management that weigh arriving alerts based on the history and past experience of their senders. Consequently, an

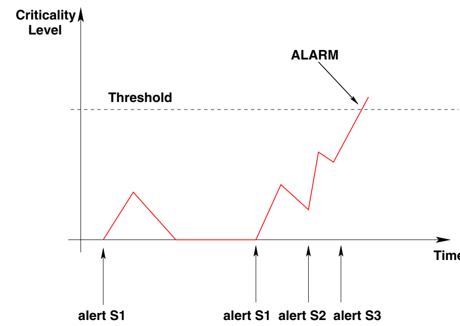


Fig. 3. Criticality level evolution in time. Alerts are raised by sensors S1, S2 and S3 that may be of different types but correlated. An alarm is raised only if the threshold is reached

alert can contribute less in the criticality level if it earns a bad reputation. Due to space constraint we do not explain in this paper how the reputation is maintained and updated dynamically at the management node.

## IV. Preliminary Results

In order to validate our proposed management scheme we simulate an area monitoring scenario with wavesim a specifically developed simulator for WSN environments. Unlike other simulators, wavesim uses the callback programming technique and reproduces with high fidelity, sensors based on the Wavenis stack [7]. We will be deploying these types of sensors in a real area surveillance application hence the choice of the technology. In the wavesim simulator, the whole communication architecture we developed for our project was integrated, we skip these details here for space constraints.

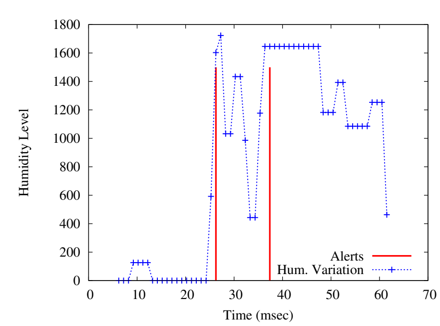


Fig. 4. Humidity level variation and alert at a sensor node

First we validate the reasoning functions implemented in each sensor node. The objective of our simulation is to show that our management scheme allows to reduce considerably the number of sent alerts to the management nodes while being highly reliable. We consider here a single humidity sensor deployed in an area and generate two major events that should trigger alerts. Figure 4 shows clearly that our reasoning techniques (whose functioning is described in Figure 2) capture correctly the environment variations. Indeed, even though the second event lasts for a long duration, a single alert is sent to the management node for each occurring phenomenon thus reducing energy consumption while capturing correctly variations in the monitored area. Note here that the threshold for sending alerts is 1500, hence our reasoning sends 2 alerts despite the fact that the node sensed 7 values higher than the defined threshold; that is nearly 75% less sent messages.

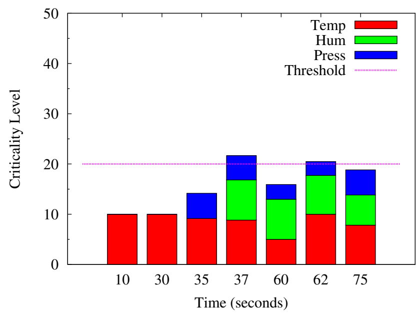


Fig. 5. Criticality level management at the management node

After validating the reasoning at the sensor level, we simulate a realistic area monitoring scenario. We deploy 10 nodes (randomly chosen between temperature, humidity and pressure sensors) within a 200 square meters area. In this configuration, all nodes are within the communication range of each others. A single node was elected to serve as management node. Dependency between nodes was coded in the reasoning node thus we assume that the learning phase was already accomplished. We fix the criticality level threshold and generate dependant and independent events in the network in a simulation of 80 seconds. This simple scenario was selected in order to keep tractability of the obtained results, we are now working on more complex scenarios, longer simulation runs as well as dynamically learning the environment in the training phase. Obtained results are shown in Figure 5. The figure shows the evolution of the criticality level at the reasoning node upon receiving alerts from the different types of sensors. Two alarms are raised to the administrator at the $37^{th}$ and $62^{nd}$ seconds. Note here that the shown alerts are at the management node level after every node locally has already filtered the messages to send to the reasoning node. The 3 types of alerts contribute together in increasing the criticality level. It is important to notice that each alert does not contribute with the same percentage in the criticality level. This is due to the fact that a different number of sensors of each type are deployed in the network, and furthermore because each type of sensed data was assigned a particular weight while computing the criticality level. The notion of node reputation was not simulated here, it is in our future work list. The created redundancy in the number of sensors and in the type of sensed data has the advantage of increasing the reliability of our reasoning scheme. Indeed, our management technique by limiting the number of alerts sent by each node reduces the bias that may be caused by corrupted nodes and generates alarm if dependant events in other nodes occur. Figure 5 highlights also the fact that the criticality level decreases (linearly) with time. Consequently, if no other dependant alerts arrive in the dedicated period of time the criticality level goes back to its initial value. In summary, our management scheme reduces the number of alarms sent to the control center by combining intelligently received alerts. Moreover, relying on the created dependency between events helps ensure reliability in detection as well as reduced energy consumption.

## V. Related Work

Few research proposals have already used automated reasoning tools in wireless sensor networks with the objectives of intelligent management and network lifespan extension. Krishnamurthy *et al.* propose RESTORE [5], an event correlation and storage service for WSN. RESTORE divides the network into zones with a manager in every zone. The manager correlates information arriving from nodes within its zone. It has also a storage capability to keep track of these events. The objective of RESTORE is to distribute within each zone detected events and to store most important ones. However, our work mainly differs from this proposal in the way we correlate information and build the dependency tables. In fact, in our case the correlation is not based on geographic proximity but on a built dependency through a Bayesian reasoning in the training phase. Moreover, by introducing the reputation management concept, our management scheme enables the correlations to evolve by giving low impact and even removing in the criticality level computation nodes whose reputation is very low. Spatial and geographical correlation was also exploited in WSN to propose efficient MAC protocols that reduce contention. More precisely, authors in [8], [9], and [10] correlate information from sensors situated in the same geographic zone with the objective of deactivating nodes (putting in sleep mode) that detect the same event. This strategy reduces contention on the wireless medium by making a single sensor report every event. Our approach is completely different since in our case redundancy in detected events is necessary to add reliability to our system and make it operate autonomously.

## VI. Conclusion and Future Research

In this paper we have presented a management scheme for area monitoring in wireless sensor networks. Our scheme ensures reliable monitoring while reducing considerably the energy consumption of sensor nodes. By using reasoning services from the artificial intelligence field, we reduce the number of exchanged messages by raising alarms to the network administrator only if correlated events occur in the same time. Our solution can be used for variant types of surveillance application such as intrusion detection in parks, villas and military camps. It can also be used for weather and climate monitoring applications.

We are currently implementing in wavesim the reputation management at the reasoning node. By maintaining and dynamically managing the reputation of each active sensor, reasoning node one can isolate malicious sensors. Moreover, we are focusing on optimizing the learning phase and on learning and adapting dynamically the thresholds required for the management functions.

## REFERENCES

[1] K. Kalpakisand, K. Dasgupta, and P. Namjoshi, "Efficient algorithms for maximum lifetime data gathering and aggregation in wireless sensor networks," *Elsevier computer networks*, 2003.
[2] J. Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," *IEEE/ACM transactions on Networking*, 2004.
[3] W. Ye and J. Heidemann, "Medium Access Control In Wireless Sensor Networks," *Wireless Sensor Networks, SpringerLink*, 2004.
[4] M. Alessandra, M. Davide, and B. Roberto, "Non-monotonic reasoning supporting wireless sensor networks for intelligent monitoring: The sindi system," in *LPNMR*, 2009.
[5] S. Krishnamurthy, T. Hie, G. Zhou, J. Stankovic, and S. Son, "RESTORE: A Real-Time Event Correlation and Storage Service for Sensor Networks," in *IEEE INSS*, 2006.
[6] A. Glenberg, "Learning from data : an introduction to statistical reasoning." *Taylor & Francis*, 2008.
[7] http://en.wikipedia.org/wiki/Wavenis.
[8] M. Vuran and I. Akyldyiz, "Spatial correlation-based collaborative medium access control in wireless sensor networks," *IEEE/ACM Transactions on Networking*, 2006.
[9] G. Zheng and S. Tang, "Spatial Correlation-Based MAC Protocol for Event-Driven Wireless Sensor Networks," *Journal of Networks*, 2011.
[10] G. Shah and M. Boyzigit, "Exploiting energy-aware spatial correlation in wireless sensor networks," in *IEEE COMSWARE*, 2007.