

# CONCEPTS AND EVOLUTION OF RESEARCH IN THE FIELD OF WIRELESS SENSOR NETWORKS

Ado Adamou ABBA ARI <sup>1,3\*</sup>, Abdelhak GUEROUI <sup>1</sup>, Nabila LABRAOUI <sup>2</sup> and  
Blaise Omer YENKE <sup>3</sup>

<sup>1</sup> PRISM, University of Versailles St-Quentin-en-Yvelines, France

<sup>2</sup> STIC, University of Tlemcen, Algeria

<sup>3</sup> LASE, University of Ngaoundere, Cameroon

## ABSTRACT

*The field of Wireless Sensor Networks (WSNs) is experiencing a resurgence of interest and a continuous evolution in the scientific and industrial community. The use of this particular type of ad hoc network is becoming increasingly important in many contexts, regardless of geographical position and so, according to a set of possible application. WSNs offer interesting low cost and easily deployable solutions to perform a remote real time monitoring, target tracking and recognition of physical phenomenon. The uses of these sensors organized into a network continue to reveal a set of research questions according to particularities target applications. Despite difficulties introduced by sensor resources constraints, research contributions in this field are growing day by day. In this paper, we present a comprehensive review of most recent literature of WSNs and outline open research issues in this field.*

## KEYWORDS

*WSNs, protocols, sensor, applications, routing, services, survey, bio-inspired.*

## 1. INTRODUCTION

During last decade, the field of WSNs has attracted the attention of scientific and industrial community. With this particular kind of ad hoc networks, it is possible to perform various applications grouped into monitoring and tracking of some activities. The rapid evolution of the Micro-Electro-Mechanical Systems (MEMS) has contributed to the development of small and smart sensors [1]. These sensors have become increasingly very small in terms of size, more intelligent and less expensive [2]. A node in WSN consists of a sensor unit, a processing and data storage unit, a wireless transmission module and a power management unit. Each node is able to gather and process physical information in order to transmit these data to a base station or sink node. WSN consists of a deployment of one or more sink nodes and a number of sensor nodes in a physical environment.

Wireless sensors are designed with huge resource constraints: a limited amount of energy; reduced computing capacity; limited memory size and storage; short-range of communication and reduced bandwidth. So, it appears some problems in networks architectures, QoS (Quality of Service), coverage, security, fault tolerance, etc. [3]. In a WSN, energy consumption depends of network architecture, environment in which the network is deployed and the underlying

application. WSNs have many applications in environmental monitoring, prevention of natural disasters, military sector, in the medical, bio-medical and veterinary field, in commercial area, especially in supply chains, aviation and automotive safety, in field of distribution of energy and in agriculture [5, 6, 7, 8, 9, 10].

In general, research papers present specific results or reviews of specific research area. The novice who is engaged in the study of WSNs does not have a panoramic view of the ongoing and forthcoming works in the field of sensor networks. It is, therefore, important to provide an overview of main concepts, and also the evolution of the research. The main motivation of this paper is to provide a comprehensive overview of the field of WSNs, its evolution and actual research issues.

The research WSN domain is constantly evolving as evidence by publication of several contributions, but improvement is still possible and some challenges remain open: location, timing, coverage, energy management, security, synchronization aggregation and data compression. This paper sets out to present a brief survey in the field of WSN.

The rest of this paper is organized as follow: in section 2, we provide some most recent survey of WSNs and highlight the originality of this review, Section 3 present sensors and types of sensor networks; in section 4, we discuss on architectures, offered services and fault tolerance; in section 5, some practical applications of sensor-based network are presented; section 6 present a review of some communication protocols and a comparison of them is proposed; section 7 describes sensor network security and some challenges are introduced; section 8, discusses on open research issues and section 9 concludes the paper.

## **2. RELATED WORK**

A top-down approach is followed by authors in [61], in order to give an overview of several applications of sensor networks. Also, they present an overview of key issues of WSNs and review literature of some aspects by classifying the problem into three groups. They review the major development of internal platform and its underlying operating system, communication protocol stack, and network services, provisioning, and deployment. In addition, these authors provide a discussion on the new challenges in the field of sensor networks.

WSNs target applications need a number of requirements which include range, antenna type, target technology, components, memory, storage, power, lifetime, security, computational capability, communication technology, size and programming interface. Interested readers may refer to the survey proposed in [4], in order to have information about some commercial and research sensors prototypes based on the above parameters. A comparison of presented sensors technologies against their addressable range, computational capability and storage capacity is provided in [4].

Researchers have provided a number of various contributions in order to achieve a large scale deployment and widespread management of WSNs in real applied domains. A recent applications of WSNs are highlighted in [69]. Authors propose the most recent technologies and testbeds for sensor networks which introduce appreciable synergies with others technologies. Based on that, they identify several challenges that need further investigations. In the same order, a selection of best testbeds applications of WSNs that have been developed for sensor evaluation is reviewed in [70].

Regarding consumption, the key challenges in WSNs is to maximize network lifetime while minimizing energy consumption. Techniques that allow the minimisation of energy wastage and the increasing of network lifetime by balancing the energy level of all nodes in network is reviewed in [62]. In the same order of ideas, the authors of [63] survey the main techniques used for energy conservation in sensor networks. They focused on duty cycling schemes that represent the most compatible technique for energy saving, data-driven approaches that can be used to improve the energy efficiency and on review of some communication protocols.

Limitation of resources in sensor nodes, security mechanism are difficult to implement in wireless sensor network. Because of that, it is necessary to neutralize attacks on all layers of sensor network protocol. More secured protocols are proposed [25, 27, 67, 68], but most of them introduce a lot of network overhead. An investigation of overhead due to the implementation of some common security mechanisms is given in [64]. Hence, providing a trusted WSNs remains a big challenge. A survey of some sensor networks security protocols is proposed by authors in [65, 66].

Except [61], which proposes an overview from application to physical layer, all of above presented survey are focused on a given aspect of sensor networks. Our survey is different from most proposed surveys in the literature in that, we discuss on all aspects and outlook of WSNs. We provide a comprehensive tool to get an overview and promising directions in sensor networks such as bio-inspired solutions which provide optimal methods for good management in sensor networks. To achieve that, we focused on most recent work in the literature.

### **3. SENSORS NETWORKS**

A wireless sensor is a veritable embedded system with a wireless communication function, and that is capable to:

- Collect physical quantities such as heat, humidity, temperature, vibration, radiation, sound, light, movement, etc.
- Convert them into digital values which are sent as sensed data to a remote processing station or base station.

In general, there are two types of sensors: general's sensors and gateways sensors. A generic sensor has a role of collecting measures from the deployment area while the gateway sensor has more capacity in terms of computing resources, storage and transmission. Gateways sensors are generally used in a particular type of WSN architecture. A general architecture of WSN is given in figure 1.

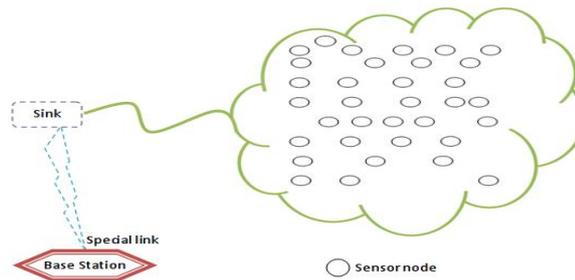


Figure 1. General architecture of WSN.

### 3.1. Wireless Sensor Networks

A WSN meanwhile can be defined as an adhoc network especially consisting of a number of wireless sensors that are deployed on a given area, to ensure an accurate task, either for monitoring or for tracking or for both. In [11], authors describe some aims of WSN design as following:

- self-organization, auto-recovery of faults, autonomous detection and correction of intrusions;
- scalability, adaptability, reliability and cooperative effort of sensor nodes;
- low power consumption, low node cost;
- routing, fault tolerance, QoS, security;
- survival to a change of topology in case of arrival and departure of node;
- survival to resources constraints.

Each sensor has an operating system. TinyOS is the specifically operating system designed for sensors and is thereby the most used [12, 13]. It's an event-driven operating system which provides a framework for programming embedded systems. The middle-ware proposed by TinyOS supports synchronization, routing, data aggregation, localization, radio communication, task scheduling, I/O processing, etc. Moreover, there are other sensors operating systems more or less popular: SOS cormos, EYES, PEEROS, MantisOS, Contiki, Kos, Senos, Nano-RK, LiteOS [14].

Particular type of ad hoc networks, WSNs have some differences with common ad hoc networks. Indeed, the number of nodes in a WSNs is more large (one to several thousand) and nodes are generally static and cooperate together to move gathered data towards the base station. In classical ad hoc networks, there are fewer nodes, but there's higher mobility. In terms of communication, WSNs have broadcasting mechanism throughout the network while classical ad hoc networks make the point to point communication. Also, in terms of energy consumption, it is lower in WSNs [15].

### 3.2. Types of WSNs

Depending on the deployment environment on earth, underground or underwater, there are several types of wireless sensor network.

- **Terrestrial:** In this type of sensor networks, hundreds to thousands of sensors deployed randomly or pre-deployed on a given area. This type of WSNs is mainly used in the field of environmental monitoring and presents a challenge to the sustainability of the network in terms of management of energy [16].
- **Underground:** These very special sensor nodes are known for their high cost and the required logistics for maintenance and pre-planned deployment. Sensors are installed in the soil for agriculture or in the walls of a mine to monitor conditions in the soil. However, in this type of network, there is land node which has role of relaying sensed information by the underground nodes to the base station [17].
- **Underwater:** This type of WSNs are still a great research challenge because of fact that environment in which the nodes are deployed is hostile and usually used for exploration. It's only possible to deploy a few nodes, these nodes are more expensive than terrestrial sensors, wireless communication is acoustic, the bandwidth is limited, the loss of signal is recurrent, propagation delays and synchronization problems are high [4, 19].
- **Multimedia:** This type of WSNs allows monitoring of a tracker in real-time events such as images, videos and sound. These sensors are equipped with cameras and microphones. Importance is given for: good bandwidth which implies a high energy consumption; processing and data compression; good QoS. Advance planning is necessary for the deployment of these sensors [20].
- **Mobile:** In this most recent type of WSNs, nodes are capable of repositioning and autonomously reorganize the network. After initial deployment, nodes disperse to collect information. There's also a hybrid network that consists of the combination of mobile sensors and fixed sensors [21].

#### **4. ARCHITECTURE, OFFERED SERVICES AND FAULT TOLERANCE**

Architecture of sensor network depends of expected service and the implemented application.

##### **4.1. Architectures**

Several sensor models are offered according to the underlying application. In general, a sensor node has: a sensor unit whose role is to capture a physical quantity and transform into a digital value; a data processing and storage unit; a wireless transmission module; a unit of management and control of energy. Also, depending on the application, some modules are added: GPS, solar cell, etc. Figure 2 present general node architecture.

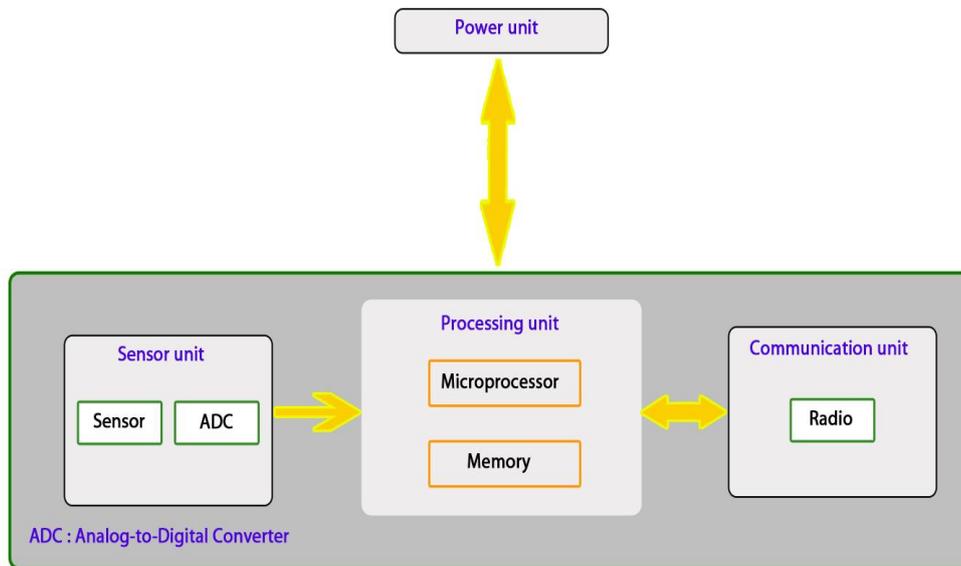


Figure 2. Sensor architecture.

There are two main types of network architectures for WSNs: (1) flat architecture, (2) hierarchical architecture.

1. In **flat architecture**, except for sink node, the other nodes are identical, they have the same capacity in terms of energy and computing, Also, they have the same role in sensing task. Node can directly communicate with a sink in single hop manner or communication with sink can be in multi hops manner. Simplicity presented by this architecture enables low communication latency. Furthermore, when the network becomes denser, the scaling problem arises mainly as regards routing. Figure 3 present WSNs flat architectures.
2. A **hierarchical architecture** to deploy a large number of sensors. The network is divided into several groups or clusters which are the organizational unit of the network. Depending of cases, a more expensive cluster node type and more powerful than other nodes or a normal node in the cluster is designated as group leader called cluster head that is responsible of coordination of the sensors under its responsibility and act as a gateway to another cluster. The cluster head is responsible for the aggregation and/or compression of all the collected data in order to route it to the sink [22]. This allows the reduction of the transmission data within the network. However, there may be more latency in communications due to the density of the network and higher energy consumption for the cluster heads. Figure 4 highlight the clustered architectures for multi hops and single hop clusters.

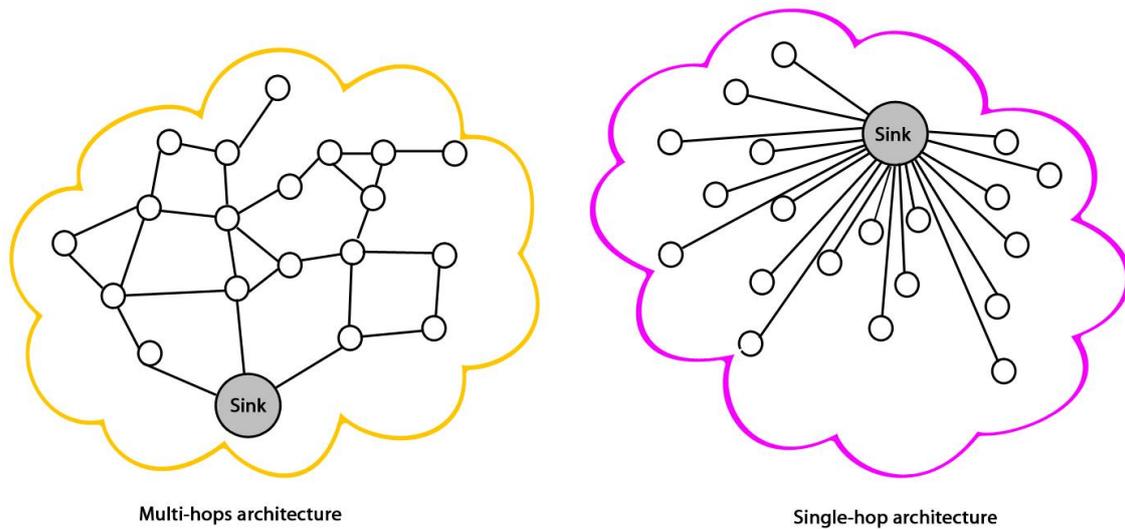


Figure 3. WSNs flat architectures.

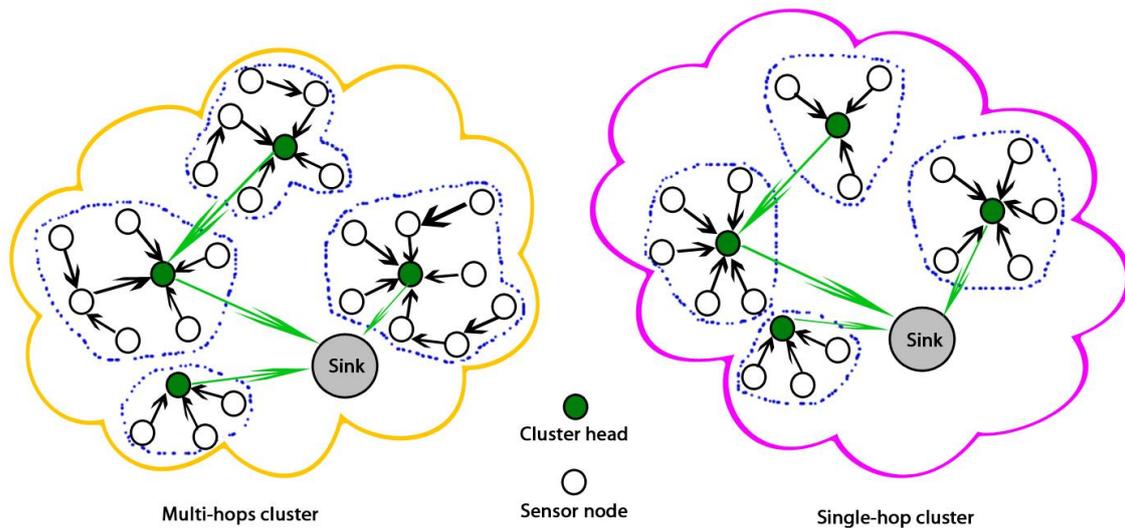


Figure 4. WSNs hierarchical architectures.

## 4.2. Offered services

Offered services in WSNs are organized into provisioning, control nodes management. Coverage and localization are the provisioning services. Control and nodes management enable WSN middle-ware to deliver services such as security, synchronization, compression and data aggregation.

1. **Coverage:** It involves the placement of nodes in deployment area to ensure coverage of the entire area by the network [28]. Coverage depends of application, the number of nodes and localization of these nodes.

2. **Localization:** It consists of finding position of a node in the network. In sensor network, three methods of localization are usually used [27] : - GPS (Global Positioning System) is the easiest, but cost of energy consumption is high and can't work on dense environment as forest; - anchor nodes approach which consist of node called anchor whose knows its position and help its neighboring nodes to evaluate their own; - close localization which consist of a node that using the neighboring nodes to determine their positions and then become an anchor node to other nodes.
3. **Synchronization:** Allow the realization of an activity or process at the same time as other nodes is an important service in WSNs. Synchronization is very important especially for routing and energy saving [26].
4. **Data compression:** It reduces the cost of communications and increase the reliability of data transfer. Compression involves the strict reduction of the amount of data to be routed towards the base station. Data compression requires decompression, which can reproduce compressed data in their original format. Decompression is achieved at the base station [24].
5. **Data aggregation:** It can greatly help to conserve the scarce energy resources by eliminating redundant data, thus achieving a longer network lifetime [23]. In other words, data aggregation is usually achieved by cluster head and consists of collecting data from all cluster members, applying an aggregation function to all collected data and transmits just one value as measured data.
6. **Data and network security:** WSNs are vulnerable to attack that consist of compromising a node, alter the integrity of the data, listening the network to retrieve messages or inject false messages in order to create a wasted of resources. Despite the difficult task of properly securing a WSN because of the significant limitation of resources, security protocols exist and ensure the security service nodes and network [22, 25].

### 4.3. Fault tolerance in WSN

Constraints in terms of resources capacities and the hostility of deployment environments expose WSNs to multiple to failures. Interactions with the environment or the deployment area may be the cause of network failures or any part of it. For a good scheduling operation, the network must be fault tolerant because sensors can have manufacturing error, lack of energy or victim of a security attack.

The aim of fault tolerance in WSNs is for example to achieve the network scheduling even if there's a node failure. In other words, fault tolerance in sensor network can be seen as ability to maintain network running without interruption in presence of failure of a sensor node. Fault tolerance is generally implemented in routing and transport protocols. It consists in the realization of the following two steps: detection of failure and limitation of effect; recovery and treatment of failure [38].

In particular, large-scale sensors networks are more exposed to failures because of inhospitable nature of their deployment environment. So restoring network after a damage is needed. According to this, authors in [60] propose a strategy for achieving fault tolerant network by establishing a bi-connected inter-cluster topology. The simulation of their approach shows a result in term of network connectivity.

In [39], a study of fault tolerant relay node placement problems is achieved and also discussion about complexity of proposed modified algorithms is done. In [40], authors present an artificial neural network model for fault tolerant WSN. A fault tolerant QoS clustering approach for WSNs is proposed in [41]. The use of dual cluster head mechanism guarantee the QoS, but some introduce security problem.

## 5. APPLICATIONS

The rapid evolution of sensor technology has led to design very small and smart sensors, which are used for various applications. Selection of a given type of sensor depends of desired application [29]. In fact, each application of WSN has a set of requested requirements as coverage, location, security, lifetime, etc. Classification of WSNs application can be mainly done into two categories: monitoring and tracking. In figure 5 we summarize this classification.

### 5.1. Monitoring

Monitoring is used to analyse, supervise and carefully control operations of a system or a process in real-time. Sensor network-based monitoring applications are various. Below some of them are briefly presented:

- **Environment:** monitoring of water quality, weather, pressure, temperature, seismic phenomena, vibration, monitoring of forest fires.
- **Agriculture:** irrigation management, humidity monitoring.
- **Ecology:** monitoring of animals in their natural environments.
- **Industry:** supply chain, inventory monitoring, industrial processes, machinery, productivity.
- **Smart house:** monitoring any addressable device in the house.
- **Urban:** transport and circulation systems, self-identification, parking management.
- **Health care:** organs monitoring, wellness, surgical operation.
- **Military:** intrusion detection.

### 5.2. Tracking

Tracking in WSN is generally used to follow an event, a person, animal or even an object. Existing applications in the tracking can be found in various fields.

- **Industry:** traffic monitoring, fault detection.
- **Ecology:** tracking the migration of animals in various areas.
- **Public health:** monitoring of doctors and patients in a hospital.

- **Military:** a WSN can be deployed on a battlefield or enemy zone to track, monitor and locate enemy troop movements.

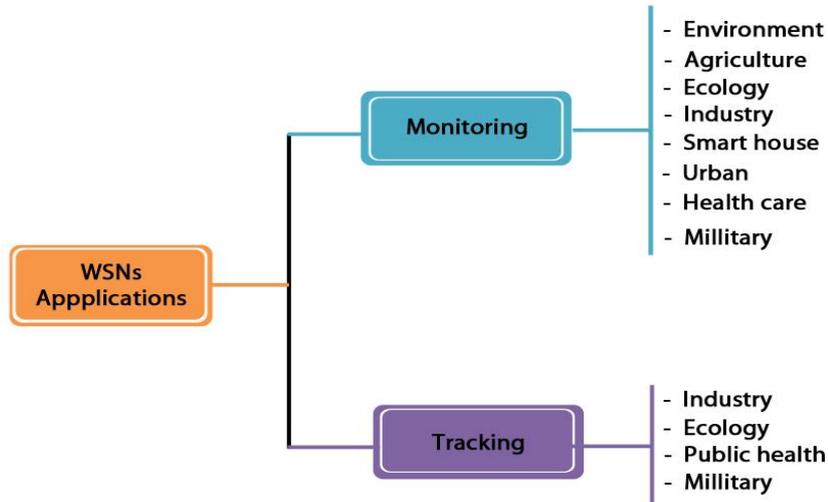


Figure 5. Classification of WSNs Applications.

### 5.3. Some practical applications

Precision agriculture is based on detailed processes of crop conditions such as the degree of fertilization, pesticide use or even crop protection against insects. A case of using WSN to achieve these advanced agricultural techniques was done in the south of Italy to produce tomatoes in a greenhouse. In fact, a sensor network is deployed for reducing pesticide usage in order to preserve environment and maximize the quality of tomatoes. The first application focused on measuring micro-climate of tomatoes crop to deliver detailed information for a novel decision system that help farmers to improve the quality of their production [30]. To deploy the WSN, Sencicast system is used and for management of network, the SensiNet platform was used [31].

In [32], authors present a case of using sensors in supply-chain for tracing transportation of perishable food. Indeed, to avoid the loss due to rotting in transportation, temperature sensors are deployed in trucks and other radio mechanisms called RFIDS are used for sending data and location to a remote site. In [33], authors has done an investigation of potential of sensor-based issuing policies such as FIFO, LIFO, SIRO, HQFO, LQFO, etc. on product quality in the perishables supply chain. In the same idea, authors in [34] have developed a real-time ZigBee based WSN for monitoring to the perishable food supply chain management. They also present their system architecture, hardware design and software implementation. The result shows a good network lifetime and high success rate in data transmission.

Sensors devices are also more used in medical monitoring system in order to improve health care of patients. There is a need of sensing applications in order to improve efficiency and quality of care in hospital environments. In [35], authors has deployed a WSN to monitor heart rate and

blood oxygen levels at emergency room of a hospital and they use these data to know about the performance of hospital. Despite multiple frequency channels in hospital environment, their application achieve a good routing and high data reception rate.

Because climate change is a real problem for our planet, environmental monitoring become is an important goal. WSN is a domain which can provide solutions for real-time monitoring of environmental parameters as temperature or pressure in urban, rural, mountain or maritime zone. A case of study micro-climate phenomenon on top of a rock glacier in Switzerland by using WSN is described in [59]. Because of long-term experience nature of their project, authors have deployed a number of sensors with sufficient energy resources by adding secondary battery and solar panel. Environmental quantities measured by their WSN are: air humidity and temperature; precipitation; soil moisture; solar radiation; surface temperature; water content; wind direction and speed.

An application of sensor technology for environmental health monitoring in urban environments has been studied by authors in [36] for specific case in Nigeria country. Because of much environmental pollution in region of Niger Delta, authors have developed bio-monitoring approaches to study impacts on certain organisms. In the same idea, a study of monitoring water quality in urban reservoirs is presented in [37]. Authors propose an optimal sensor placement scheme to measure the wind distribution over a large urban reservoir with a limited number of wind sensors.

## 6. COMMUNICATION PROTOCOLS

The communication protocols in WSNs are different from traditional communication protocols because of the strong limitation sensor resources [18]. These protocols are based on five layers: application, transport, network, link and physical. Depending on the gathered value, software is able to exploit data from application layer in order to compute and interpret the collected data. The transport layer ensures the reliability and quality of data between source and destination. Network layer in collaboration with transport layer, has a role of routing data across the network. The link layer allows detection and error correction, and contributes to the reduction of the collision of messages in the network. The physical layer provides an interface to send/receive byte stream to/from the communication channel.

Network protocols depend largely on the transport protocol. Implementation of transport protocol must be general and independent of the application. Transport protocol manages congestion in the network, transmission reliability and ensures energy conservation. In the field of WSNs, routing data from a source to a destination is a task that requires a build of fault tolerant, secure and fairness protocol [29]. Routing protocol in WSNs can be categorized in four groups: Data-centric protocol; Hierarchical protocol; Location-based protocol and Bio-inspired protocol.

**Data-centric protocols:** The main concept implemented by these categories of network protocol is to control and eliminate redundant data in the network.

**Hierarchical protocols:** These kinds of protocol are generally designed for large scale WSNs. Nodes are organized into clusters. Each cluster head is responsible to aggregate data for transmission to the base station. This is done in order to reduce the energy consumption of sensor nodes.

**Location-based protocols:** These protocol categories use the position information to send the data only to the desired destination.

**Bio-inspired protocols:** These types of routing protocol are more recent. It consists of using analogies between computing methods and biological behaviors of swarms in which collective intelligence can emerge. These swarms are colonies of social insects, bird flocking and fish schooling, firefly, etc...

In table 1, we present a comparison of some routing protocols.

	Routing	Scalability	Synchronization	Coverage	Data aggregation	Security	Overhead	Energy-consumption	Maintenance
<b>HEERP [42]</b>	Hierarchical	yes	yes	-	yes	-	less	less	yes
<b>EADC [43]</b>	Hierarchical	yes	yes	yes	yes	-	less	less	-
<b>U-LEACH [44]</b>	Hierarchical	yes	yes	-	yes	-	less	less	
<b>ALS [45]</b>	Location-based	yes	no	-	no	no	medium	-	-
<b>[46]</b>	Location-based	yes	no	-	no	no	medium	-	-
<b>MSDD [47]</b>	Data-centric	no	yes	yes	no	no	medium	less	yes
<b>[48]</b>	Data-centric	no	no	no	no	no	high	high	-
<b>[49]</b>	Data-centric	no	no	no	no	no	medium	less	-
<b>[50]</b>	Bio-inspired	yes	no	yes	yes	-	less	less	yes
<b>[51]</b>	Bio-inspired	yes	no	yes	no	-	less	less	yes

## 7. SECURITY IN SENSOR NETWORKS

In order to design a WSN application, it is supposed that all sensor nodes are each other worthy of trust. However, sensor nodes are generally deployed on uncontrolled and inhospitable environments. This situation exposes the sensors to different kinds of attacks that can totally damage network operations. Indeed, these attacks mainly exploit the uncertainty of the communication channel and the random deployment of sensors on an uncontrolled area. Thus, ensure the safety of this type of network is a difficult task, especially because nodes have limited hardware capabilities [71].

Security in WSNs can be classified into two broad categories: operational security and information security. The security of WSNs can be classified into two broad categories: QoS and security. The first category aim to ensure the continuity of operations in the entire network, even if, there is a faulty node or if a node was attacked. For the second, the objective is to ensure data confidentiality, integrity, authentication, availability and freshness. In fact, an attacker can compromise a sensor node by altering the integrity of the data, injecting fake data on the network or eavesdropping. These attacks are commonly partitioned into physical and logical vulnerabilities.

Physical vulnerability is a kind of attack in which an adversary alter a part of sensor, such as changing its programming code or replace a given sensor by a compromised node. Logical vulnerabilities lie in the programs and protocols. Furthermore, some attacks intended to affect the integrity of messages that pass through the network, while others are designed to reduce the availability of the network or its components. These attacks are in two kinds: passive and active.

In passive attack, the goals of adversary is to collect information in the network without being discovered [72]. This is possible because of technology of wireless communication channel. In fact, transmissions are broadcast by radio waves, no network access control is possible. The most known attack based on that is called eavesdropping. Therefore, it's very easy to intercept exchanged data and analyse the traffic if there is no planned privacy service.

Active attacks are more harmful than passive attacks, for network operations and lifetime. When an attacker successfully compromises the network, he can modify messages, introduce unneeded traffic in order to exhaust node energy. In this range are Wormhole, Sybil and Sinkhole attack, that are known as routing attack because they act on network layer [72]. Details of attacks per layer can be found on [72, 73]. In the same order of harm, Denial of Service (DoS) attacks which consist of sending an unlimited number of messages in order to exhaust resources, are implemented in different layer of protocol stack.

Due to resources limitation, it's therefore necessary to design new robust algorithms to carry out routing operations even in the presence of malicious nodes. In addition, securing data aggregation operations and node localization schemes remains a challenge. Even so, various solutions are proposed for designing secure sensor networks [23, 68, 75]. Also, bio-inspired techniques promise an outlook for secure sensor networks. For example, a bio-inspired cryptographic algorithm for WSNs based on genetic programming is proposed in [74].

## **8. OPEN RESEARCH ISSUES**

In general, the challenges are the designing of WSNs by taking in account of limited energy capacity, resources constraints, random and large deployment, dynamic and not controlled environment. In this section, we propose a small discussion about the opened research issues in terms of services, applications, fault tolerance and communication protocols. Also, discuss on bio-inspired solutions which promise a good perspective in fields of WSNs.

Current localization algorithms still have a considerable cost in terms of energy consumption [27]. It's therefore, necessary to design energy efficient localization algorithms and techniques. Promising nature-inspired approaches for nodes localization are proposed in [52, 53]. The proposed algorithms show a little gain in term of energy consumption, but improvement remain possible.

In another hand, WSN services such as coverage, synchronization, collision control, data aggregation and compression, are still a challenge which need particular attention for better improvements. Detection and response to an attack without interrupting the operation of the network is a challenge for secure networks. In particular, for security issues and because data is the final need by applications, secure data become much important for on top applications. In fact, a compromised node may send arbitrary data and delude the sink node. In [2], a robust adaptive approach based on hierarchical monitoring providing trust data aggregation is proposed to secure data received by the base station. Also, secure all WSNs services remain a big challenge because of sensor resource constraints.

Otherwise, the rapid development of wireless sensor technology is mainly due to the different needs of applications. Also, each sensors networks application is specific to a given domain. Therefore, there is a need of development of application solutions by taking in account of specificities of concerned domain. These specificities must meet the constraints of sensor technology and therefore this leads to research questions.

Enable reliable communication while managing congestion in the network is the main challenge of the transport layer on sensor protocol stack. In terms of network protocols, several are offered depending on the considered sensor network architecture. However, fairness, reliability, congestion control and overhead are still problems to solve in network protocols [54]. In order to optimize network protocols, introduction of cross-layer approach are proposed for WSNs. In fact, interaction between all layers of the protocol stack may optimize sensors performances and so cross-layer optimization becomes an important research direction for sensor network. A case of optimizing communication protocol by using cross-layer optimization combined with a Markov chain model is proposed in [55].

Moreover, bio-inspired solutions are progressively applied in WSNs [50, 51]. Swarms intelligence, artificial immune system, genetic algorithm and other nature-inspired phenomenon in which self-organization and collective intelligence can emerge, are increasingly used in the fields of sensor networks in order to optimize the whole management of WSNs [56, 57, 58]. We believe that more nature-inspired applications and models will be proposed in the near future and this will provide a good progress in WSN.

## 9. CONCLUSION

WSNs offer great opportunities for diverse applications. This technology and existing applications are constantly growing. Also the research in this field is very exciting because of a variety of offered services by sensors networks. In this paper, we present a review of WSNs by highlighting some aspects of this particular type of ad hoc networks, and open research directions in this field. Nevertheless, several problems still require improvements, despite the number of contributions. In particular, security, localization, energy efficient intelligent routing, etc. remain open. Also, we made a small discussion about the promise of biological inspired solutions which provide a good management of sensor network. We believe that bio-inspired solutions constitute an interesting area for further research for optimizing WSNs services.

## REFERENCES

- [1] Warneke, B. A., and Pister, K. S. (2002). MEMS for distributed wireless sensor networks. In *Electronics, Circuits and Systems, 2002. 9th International Conference on* (Vol. 1, pp. 291-294). IEEE.
- [2] Labraoui, N., Gueroui, M., Aliouat, M., and Petit, J. (2011). RAHIM: Robust Adaptive Approach Based on Hierarchical Monitoring Providing Trust Aggregation for Wireless Sensor Networks. *J. UCS*, 17(11), 1550-1571.
- [3] Arampatzis, T., Lygeros, J., and Manesis, S. (2005, June). A survey of applications of wireless sensors and wireless sensor networks. In *Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation* (pp. 719-724). IEEE.
- [4] Potdar, V., Sharif, A., and Chang, E. (2009, May). Wireless sensor networks: A survey. In *Advanced Information Networking and Applications Workshops, 2009. WAINA'09. International Conference on* (pp. 636-641). IEEE.
- [5] Mainwaring, A., Culler, D., Polastre, J., Szewczyk, R., and Anderson, J. (2002, September). Wireless sensor networks for habitat monitoring. In *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications* (pp. 88-97). ACM.
- [6] Lédeczi, Á., Nádas, A., Völgyesi, P., Balogh, G., Kusy, B., Sallai, J., ... and Simon, G. (2005). Countersniper system for urban warfare. *ACM Transactions on Sensor Networks (TOSN)*, 1(2), 153-177.
- [7] Palumbo, F., Ullberg, J., Štimec, A., Furfari, F., Karlsson, L., and Coradeschi, S. (2014). Sensor network infrastructure for a home care monitoring system. *Sensors*, 14(3), 3833-3860.

- [8] Tsai, T. H., Yang, C. Y., and Chen, S. M. (2013). Development of a Dissolved Oxygen Sensor for Commercial Applications. *Int. J. Electrochem. Sci*, 8, 5250-5261.
- [9] Sarafi, A., Tsiropoulos, G. I., and Cottis, P. G. (2009). Hybrid wireless-broadband over power lines: A promising broadband solution in rural areas. *Communications Magazine, IEEE*, 47(11), 140-147.
- [10] Malinowski, J., and Geiger, E. J. (2014). Development of a wireless sensor network for algae cultivation using ISFET pH probes. *Algal Research*, 4, 19-22.
- [11] Sakshat Virtual Labs: Simulating a Wireless Sensor Network. <http://virtual-labs.ac.in/cse28/ant/ant/8/theory/> accessed on december 2014.
- [12] Levis, P., Madden, S., Polastre, J., Szewczyk, R., Whitehouse, K., Woo, A., and Culler, D. (2005). TinyOS: An operating system for sensor networks. In *Ambient intelligence* (pp. 115-148). Springer Berlin Heidelberg.
- [13] Jihua, Y., and Wen, W. A. N. G. (2014, August). Research and Design of Solar Photovoltaic Power Generation Monitoring System Based on TinyOS. In *Computer Science & Education (ICCSE), 2014 9th International Conference on* (pp. 1020-1023). IEEE.
- [14] Phani, A. M. R. V. A., Kumar, D. J., and Kumar, G. A. (2007). *Operating Systems for Wireless Sensor Networks: A Survey Technical Report*.
- [15] Basagni, S., Conti, M., Giordano, S., and Stojmenovic, I. (Eds.). (2013). *Mobile Ad Hoc Networking: The Cutting Edge Directions* (Vol. 35). John Wiley and Sons.
- [16] Jiang, F., Frater, M., and Ling, S. S. (2011, June). A distributed smart routing scheme for terrestrial sensor networks with hybrid Neural Rough Sets. In *Fuzzy Systems (FUZZ), 2011 IEEE International Conference on* (pp. 2238-2244). IEEE.
- [17] Yu, X., Wu, P., Han, W., and Zhang, Z. (2014). Overview of wireless underground sensor networks for agriculture. *African Journal of Biotechnology*, 11(17), 3942-3948.
- [18] Kim, D., Noel, E., and Tang, K. W. (2014, January). WSN communication topology construction with collision avoidance and energy saving. In *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th* (pp. 398-404). IEEE.
- [19] Jiang, J. A., Yang, Y. C., Su, W. S., Chuang, C. L., and Lin, T. S. (2013). U.S. Patent No. 8,576,665. Washington, DC: U.S. Patent and Trademark Office.
- [20] Misra, S., Reisslein, M., and Xue, G. (2008). A survey of multimedia streaming in wireless sensor networks. *Communications Surveys & Tutorials, IEEE*, 10(4), 18-39.
- [21] Tagne-Fute, E. (2013). *Une approche de patrouille multi-agents pour la détection d'évènements* (Doctoral dissertation, Université de Technologie de Belfort-Montbéliard, France).
- [22] Kumar, M., and Dutta, K. (2015). A Survey of Security Concerns in Various Data Aggregation Techniques in Wireless Sensor Networks. In *Intelligent Computing, Communication and Devices* (pp. 1-15). Springer India.
- [23] N. Labraoui, M. Guerroui, M. Aliouat, and T. Zia. (2011). Data aggregation security challenge in wireless sensor networks. *Ad Hoc & Sensor Wireless Networks*, 12(3-4):295-324.
- [24] Incebacak, D., Zilan, R., Tavli, B., Barcelo-Ordinas, J. M., and Garcia-Vidal, J. (2014). Optimal data compression for lifetime maximization in wireless sensor networks operating in stealth mode. *Ad Hoc Networks*.
- [25] Labraoui, N., Guerroui, M., Aliouat, M., and Petit, J. (2010, May). Adaptive security level for data aggregation in wireless sensor networks. In *Wireless Pervasive Computing (ISWPC), 2010 5th IEEE International Symposium on* (pp. 325-330). IEEE.
- [26] Madaan, S., Kumar, D., and Khurana, R. (2014). An Enhanced Approach for Synchronization in WSN. *International Journal of Computer Applications*, 94(17), 51-56.
- [27] Labraoui, N., Guerroui, M., and Aliouat, M. (2012). Secure DV-Hop localization scheme against wormhole attacks in wireless sensor networks. *Transactions on Emerging Telecommunications Technologies*, 23(1), 303-316.
- [28] Torkestani, J. A. (2013). An adaptive energy-efficient area coverage algorithm for wireless sensor networks. *Ad hoc networks*, 11(6), 1655-1666.
- [29] Buratti, C., Conti, A., Dardari, D., and Verdone, R. (2009). An overview on wireless sensor networks technology and evolution. *Sensors*, 9(9), 6869-6896.
- [30] Mancuso, M., and Bustaffa, F. (2006, June). A wireless sensors network for monitoring environmental variables in a tomato greenhouse. In *IEEE International Workshop on Factory Communication Systems* (pp. 107-110).

- [31] Sensicast systems. <http://www.crunchbase.com/organization/sensicast-systems> (accessed on July 2014.)
- [32] Jedermann, R., Behrens, C., Westphal, D., and Lang, W. (2006). Applying autonomous sensor systems in logistics—Combining sensor networks, RFIDs and software agents. *Sensors and Actuators A: Physical*, 132(1), 370-375.
- [33] Dada, A., and Thiesse, F. (2008). Sensor applications in the supply chain: the example of quality-based issuing of perishables. In *The Internet of Things* (pp. 140-154). Springer Berlin Heidelberg.
- [34] Wang, J., Wang, H., He, J., Li, L., Shen, M., Tan, X., and Zheng, L. (2015). Wireless sensor network for real-time perishable food supply chain management. *Computers and Electronics in Agriculture*, 110, 196-207.
- [35] Ko, J., Gao, T., and Terzis, A. (2009, April). Empirical study of a medical sensor application in an urban emergency department. In *Proceedings of the Fourth International Conference on Body Area Networks* (p. 10). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
- [36] Obinaju, B. E., Alaoma, A., and Martin, F. L. (2014). Novel sensor technologies towards environmental health monitoring in urban environments: A case study in the Niger Delta (Nigeria). *Environmental Pollution*.
- [37] Du, W., Xing, Z., Li, M., He, B., Chua, L. H. C., and Miao, H. (2014, April). Optimal sensor placement and measurement of wind for water quality studies in urban reservoirs. In *Proceedings of the 13th international symposium on Information processing in sensor networks* (pp. 167-178). IEEE Press.
- [38] Gupta, G., and Younis, M. (2003, March). Fault-tolerant clustering of wireless sensor networks. In *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE* (Vol. 3, pp. 1579-1584). IEEE.
- [39] Zhang, W., Xue, G., and Misra, S. (2007, May). Fault-tolerant relay node placement in wireless sensor networks: Problems and algorithms. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications*. IEEE (pp. 1649-1657). IEEE.
- [40] Acharya, S., and Tripathy, C. R. (2015, January). An ANN Approach for Fault Tolerant Wireless Sensor Networks. In *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2* (pp. 475-483). Springer International Publishing.
- [41] Prakash, T. S., Raja, K. B., Venugopal, K. R., Iyengar, S. S., and Patnaik, L. M. (2014, January). Fault Tolerant QoS Adaptive Clustering for Wireless Sensor Networks. In *Proceedings of Ninth International Conference on Wireless Communication and Sensor Networks* (pp. 167-175). Springer India.
- [42] Nesrine, K., and Ben Jemaa, M. (2012, June). HEERP: Hierarchical energy efficient routing protocol for Wireless Sensor Networks. In *Communications and Information Technology (ICCIT), 2012 International Conference on* (pp. 308-313). IEEE.
- [43] Yu, J., Qi, Y., Wang, G., and Gu, X. (2012). A cluster-based routing protocol for wireless sensor networks with nonuniform node distribution. *AEU-International Journal of Electronics and Communications*, 66(1), 54-61.
- [44] Kumar, N., Bhutani, P., and Mishra, P. (2012, October). U-LEACH: A novel routing protocol for heterogeneous Wireless Sensor Networks. In *Communication, Information & Computing Technology (ICCICT), 2012 International Conference on* (pp. 1-4). IEEE.
- [45] Zhang, R., Zhao, H., and Labrador, M. A. (2006, May). The anchor location service (ALS) protocol for large-scale wireless sensor networks. In *Proceedings of the first international conference on integrated internet ad hoc and sensor networks* (p. 18). ACM.
- [46] Seada, K., Zuniga, M., Helmy, A., and Krishnamachari, B. (2004, November). Energy-efficient forwarding strategies for geographic routing in lossy wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems* (pp. 108-121). ACM.
- [47] Lajevardi, A., Haghghat, A. T., and Eghbali, A. N. (2009, December). Extending directed diffusion routing algorithm to support sink mobility in wireless sensor networks. In *Communications (MICC), 2009 IEEE 9th Malaysia International Conference on* (pp. 541-546). IEEE.
- [48] AlShawi, I.S., Lianshan Yan, Wei Pan and Bin Luo, (2012, October). A Fuzzy-Gossip routing protocol for an energy efficient wireless sensor networks, *Sensors*, 2012 IEEE, 1-4.

- [49] Zhang, Y., and Fromherz, M. (2006, April). Constrained flooding: a robust and efficient routing framework for wireless sensor networks. In *Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on* (Vol. 1, pp. 6-pp). IEEE.
- [50] Karaboga, D., Okdem, S., and Ozturk, C. (2012). Cluster based wireless sensor network routing using artificial bee colony algorithm. *Wireless Networks*, 18(7), 847-860.
- [51] Zungeru, A. M., Seng, K. P., Ang, L. M., and Chong Chia, W. (2013). Energy Efficiency Performance Improvements for Ant-Based Routing Algorithm in Wireless Sensor Networks. *Journal of Sensors*, 2013.
- [52] Kulkarni, R. V., Venayagamoorthy, G. K., and Cheng, M. X. (2009, October). Bio-inspired node localization in wireless sensor networks. In *Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on* (pp. 205-210). IEEE.
- [53] Zhou, Z., Peng, Z., Cui, J. H., Shi, Z., and Bagtzoglou, A. C. (2011). Scalable localization with mobility prediction for underwater sensor networks. *Mobile Computing, IEEE Transactions on*, 10(3), 335-348.
- [54] Yuan, H., Yugang, N., and Fenghao, G. (2014, May). Congestion control for wireless sensor networks: A survey. In *Control and Decision Conference (2014 CCDC), The 26th Chinese* (pp. 4853-4858). IEEE.
- [55] Karvonen, H., Pomalaza-Ráez, C., and Hämäläinen, M. (2014). A cross-layer optimization approach for lower layers of the protocol stack in sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 11(1), 16.
- [56] Karaboga, D., Gorkemli, B., Ozturk, C., and Karaboga, N. (2014). A comprehensive survey: artificial bee colony (ABC) algorithm and applications. *Artificial Intelligence Review*, 42(1), 21-57.
- [57] Safa, H., Moussa, M., and Artail, H. (2014). An energy efficient Genetic Algorithm based approach for sensor-to-sink binding in multi-sink wireless sensor networks. *Wireless networks*, 20(2), 177-196.
- [58] Shamshirband, S., Anuar, N. B., Kiah, M. L. M., Rohani, V. A., Petković, D., Misra, S., and Khan, A. N. (2014). Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks. *Journal of Network and Computer Applications*, 42, 102-117.
- [59] Ingelrest, F., Barrenetxea, G., Schaefer, G., Vetterli, M., Couach, O., and Parlange, M. (2010). SensorScope: Application-specific sensor network for environmental monitoring. *ACM Transactions on Sensor Networks (TOSN)*, 6(2), 17.
- [60] Lee, S., Younis, M., and Lee, M. (2015). Connectivity restoration in a partitioned wireless sensor network with assured fault tolerance. *Ad Hoc Networks*, 24, 1-19.
- [61] Yick, J., Mukherjee, B., and Ghosal, D. (2008). Wireless sensor network survey. *Computer networks*, 52(12), 2292-2330.
- [62] Shelke, M. S. N., and Shinde, M. S. R. (2013). Energy Saving Techniques in Wireless Sensor Networks. *International Journal of Scientific & Engineering Research*, 4(4), 396.
- [63] Rezaei, Z., and Mobininejad, S. (2012). Energy saving in wireless sensor networks. *Int J Comput Sci Eng Surv (IJCSES)*, 3(1), 23-37.
- [64] Kumar, M., and Dutta, K. (2015). A Survey of Security Concerns in Various Data Aggregation Techniques in Wireless Sensor Networks. In *Intelligent Computing, Communication and Devices* (pp. 1-15). Springer India.
- [65] Patle, D., and Nemade, S. (2015). A Literature Survey on Different Type of Energy Efficiently Routing Protocol in Wireless Sensor Network. *International Journal of Scientific Engineering and Technology*, 4(1), 28-31.
- [66] Ravi, M., and Subramaniam, P. (2014), Wireless Sensor Network and its Security—A Survey. *International Journal of Science and Research (IJSR)*, 3(12)
- [67] Maerien, J., Michiels, S., Hughes, D., Huygens, C., and Joosen, W. (2015). SecLooCI: A comprehensive security middleware architecture for shared wireless sensor networks. *Ad Hoc Networks*, 25, 141-169.
- [68] Mishra, D. P., and Kumar, R. (2015). A Vision of Hybrid Security Framework for Wireless Sensor Network. *Indian Journal of Applied Research*, 5(1).
- [69] Rawat, P., Singh, K. D., Chaouchi, H., and Bonnin, J. M. (2014). Wireless sensor networks: a survey on recent developments and potential synergies. *The Journal of Supercomputing*, 68(1), 1-48.
- [70] Steyn, L. P., and Hancke, G. P. (2011, September). A survey of wireless sensor network testbeds. In *AFRICON, 2011* (pp. 1-6). IEEE.

- [71] LABRAOUI, N. (2012). LA SÉCURITÉ DANS LES RÉSEAUX SANS FIL AD HOC (Doctoral dissertation). University of Tlemcen, Algeria.
- [72] Sun, F., Zhao, Z., Fang, Z., Du, L., Xu, Z., & Chen, D. (2014). A Review of Attacks and Security Protocols for Wireless Sensor Networks. *Journal of Networks*, 9(5), 1103-1113.
- [73] Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications*, 35(3), 867-880.
- [74] Semente, R. S., Salazar, A. O., & Oliveira, F. D. (2014, May). CRYSEED: An automatic 8-bit cryptographic algorithm developed with genetic programming. In *Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, 2014 IEEE International* (pp. 1065-1068). IEEE.
- [75] Rico, J., Sancho, J., Díaz, Á., González, J., Sánchez, P., Alvarez, B. L., ... & Ramis, C. F. (2015). Low Power Wireless Sensor Networks: Secure Applications and Remote Distribution of FW Updates with Key Management on WSN. In *Trusted Computing for Embedded Systems* (pp. 71-111). Springer International Publishing.