A Survey of the approach in Connecting Wireless Sensor Networks to the Internet

Hend Bayoumi
Computer Engineering and
Control Systems department
Faculty of Engineering, Mansoura
University
Egypt

Hesham A. Ali
Computer Engineering and
Control Systems department
Faculty of Engineering, Mansoura
University
Egypt

Labib Mohammed
Computer Engineering and
Control Systems department
Faculty of Engineering, Mansoura
University
Egypt

ABSTRACT
Wireless Sensor Network (WSN) considered as one of the most interesting and probably the most researched areas in the field of distributed applications in the last decade. The distinctive architecture of WSNs contributed to install it in an extensive range of the most industrial applications such as surveillance, monitoring, predicted, and automated control systems which can facilitate in bridging the divide between user requirements and technologies. On the other hand, WSNs face several challenges such as dynamic topology, power consumption, fault tolerance, scalability, and security. The main objective of this paper is to introduce the basic concepts and characteristics of the WSNs, applications, challenges, and recent research directions. Moreover, in this paper a comparative analysis and discussion of the most recent interworking approaches like gateway-based, overlay-based, and outlining a set of challenges will be introduced. Also, the future direction of the different approaches for connecting WSN to the Internet will be discussed.

Keywords
Gateway; Internet of things; IOT; IOT Architecture; IP-enabled wireless sensor networks; TCP/IP Networks; WSN

1. INTRODUCTION
A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion, pollutants, etc.… and to cooperatively pass their data through the network to the main location [1]. WSNs are regarded as a revolutionary information gathering method to build the information and communication system which will greatly improve the reliability and efficiency of infrastructure systems [2].

As WSNs gaining popularity in its application dimensions, it becomes a necessity to connect this wireless network to the infrastructure based Internet [3]. This integration can be fruitful to retrieve gathered environmental data remotely and wirelessly. Wireless sensor networks, in particular, are a constraint with respect to network capacity [4]. The Internet Protocol (IP) has been designed for networks without these constraints in mind. Several important questions still remain: How should sensor networks be integrated into the Internet? How would addressing be? And what special challenges do they present to designers and implementers? The main objective of this paper is to present some views on these questions and to investigate how to adapt IP networking to the constraints of wireless sensor networks, and how to integrate IP-enabled sensor networks into the Internet.An entity registers its interest with WSNs and sensor nodes in WSNs monitor some information from the physical world and deliver interesting information to the entity [5]. Accordingly, WSNs should interwork with the Internet to build end-to-end application systems for customers. However, little attention has been paid for interworking between WSNs and the Internet. Even though there are a few researches, these schemes cannot be directly applied to WSNs due to different characteristics. Consequently, it is necessary to investigate efficient WSNs-Internet interworking architecture and protocol.

The rest of this paper is arranged as the following: Section 2 introduces the basic concept of Wireless Sensor Network WSN and the differences between WSN and traditional IP-based networks. Section 3 discusses the different applications of WSN. Section 4 presents in brief the challenges of WSN and most important researches in this area, Section 5 shows WSN communication approaches and design considerations, Section 6 introduces existing interworking approaches and their future directions, and Finlay section 7 presents the conclusion, summarize the paper and point at the future work.

2. SENSOR NETWORKS BASIC AND CONCEPTS
The task of joining WSN to the existing Internet brings with it several challenges. Any network that wishes to be connected to the Internet needs to address the question of how it will interface with the Internet Protocol (IP) [3]. The characteristics of WSN make them different from traditional IP-based networks as depicted in Table 1. Such characteristics form a set of challenges on the interconnection approaches as limited capabilities of WSN nodes where sensor nodes have limited abilities in dealing out, computing, memory, processing and most importantly in power supply. As focusing on TCP/IP, reducing the energy or power consumption is important in WSN protocols.

Table 1: Differences between traditional IP-network and WSN

Terms	Traditional IP-Based Networks	Traditional IP-Based Networks
Networking mode	Application independent	Application specific
Data flow	One-to-one	One-to-many, Many-to-one
Network lifetime	Long for decades	Short for days or months
Resource	Bandwidth	Energy,

constraints		memory
Operation	Administered	Self-configuring
Data rate	High	Low
Routing	Address centric	Data-centric

Another challenge is the possibility of absence of Global Unique IDs where SNs do not usually have predefined global unique Identification ID or addresses as in traditional IP-networks. For example, the Directed Diffusion protocol [6] performs data-centric querying and routing without the use of globally unique IDs such as IP addresses, also different Routing Protocols in both networks where WSN basically uses specific routing protocols that are suitable for it, which differences from the Internet protocol. Hence, WSN routing protocols use addressing systems that are not IP-compliant.

In WSN data-Centric routing technique is used rather than Address-Centric where it is public to issue a query to many "unknown" nodes by using named data. In contrast, the popular of TCP/IP transactions assume prior knowledge of the location of data and hence the destination address, using IP addresses and at last data flow pattern where the most common data flow in TCP/IP networks is one-to-one data flow. In WSN, other data flow patterns are very common. For example, broadcasting query from sink to some or all sensor nodes (i.e. one-to-many). Yet, retrieving query results takes a different form. This is due to many sensor nodes have the queried information and so send the required results to the sink in the many-to-one flow pattern.

In WSN the data gathered by the different nodes is sent to a sink, (as shown in figure 1), which either uses the data locally or is connected to other networks, for example, the Internet through a gateway [7]. The performance of data collection in sensor networks can be characterized by the rate at which sensing data can be collected and transmitted to sink nodes [8]. Theoretical measures that define the limitations of collection processing in sensor networks are the delay - which is the time to transmit one single snapshot to sink from sensors - and capacity for many-to-one data collection - which is the maximum data rate at the sink to continuously receive snapshots from sensor nodes [9].
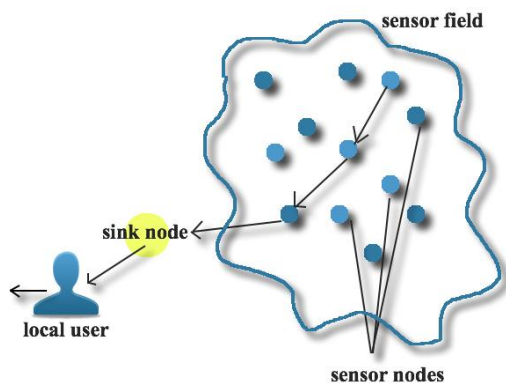

Figure 1: Data Collection process in WSN with a single Sink

3. SENSOR NETWORKS APPLICATIONS

Sensor networks may consist of different types of sensors such as seismic, low sampling rate, magnetic, thermal, visual, infrared, acoustic and radar, which are able to monitor a wide variety of ambient conditions that include the following [10]: Temperature, Humidity, Vehicular movement, Lightning condition, Pressure, Soil makeup, Noise levels, The presence or absence of certain kinds of objects, Mechanical stress levels on particular objects, and The current characteristics such as speed, direction, and size of an object [11]. The concept of micro-sensing and wireless connection of these nodes promise many new application areas. Categorized into military, environmental, health, home and other commercial areas [12].
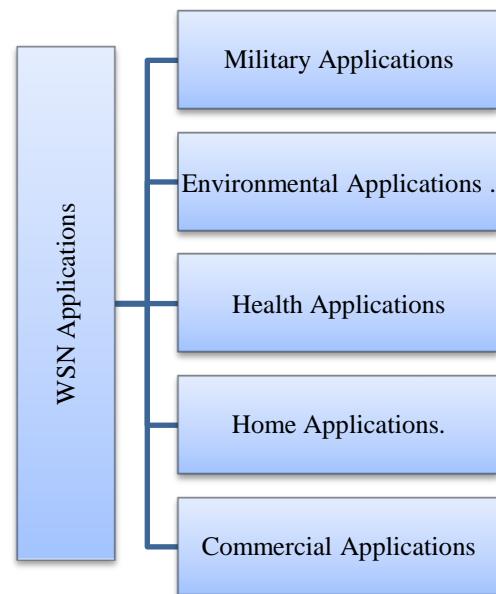

Figure 2. WSN applications

3.1. Military applications: Since sensor networks are based on the dense deployment of sensor nodes, this makes WSNs concept a better approach for battlefields. In military, sensor nodes can be used to detect, locate or track enemy movements [7]. Some of the military applications of sensor networks are monitoring the affiliate forces, equipment and reservoir, battlefield observation, enemy targeting, and nuclear, biological and chemical attack detection [12].

3.2. Environmental applications: WSNs provide the users with a better understanding of the environment in different ways such as tracking the movements of birds, small animals, and insects, monitoring environmental conditions that affect the atmospheric contexts, irrigation, monitoring soil and exploration, biological detection, forest fire detection, and flood detection [13,14]. WSNs can also be used to detect foreign chemicals in the air and the water. They can help to identify the type, concentration, and location of pollutions [15].

3.3. Health applications: A doctor can monitor the physiological data about a patient remotely to better understand the patient's current condition [12]. The medical applications can be of two types: wearable and implanted. Wearable devices are used on the body surface of a human or just at close proximity of the user. The implantable medical devices are those that are inserted inside the human body [16].

Providing interfaces for the integrated patient monitoring, diagnostics, and telemonitoring of human physiological data. Each sensor node has a specific task. For example, one sensor node may be detecting the heart rate while another is detecting the blood pressure [17].

3.4. Home applications:
As technology advances, smart sensor nodes can be buried in appliances, such as vacuum cleaners, home lights, microwave ovens, refrigerators, printers, alarm systems that cooperate with other smart devices, and VCRs [18]. The sensor nodes inside the home devices can intercommunicate with each other and with an external network via the Internet allowing end users to manage their home devices locally and remotely more easily [19]. The demand for home automation products has been increased rapidly, which promise a potential market trend in near future [20].

3.5. Other commercial applications:
Some of the commercial applications are monitoring material fatigue, product quality, constructing smart office spaces, robot control and guidance in automatic manufactures, interactive toys, interactive museums, factory process control and automation, smart structures with sensor nodes embedded inside, machine diagnosis, transportation, factory instrumentation, local control of actuators, detecting and monitoring car thefts, vehicle tracking and detection [12]. And many other applications such as toxic fume in factories detection, smart sensor systems in the car.

4. SENSOR NETWORK CHALLENGES & RECENT RESEARCH DIRECTIONS

Wireless sensor network technologies have the potential to change people's lifestyle with different applications in fields such as healthcare, entertainment, travel, retail, industry, dependent care, and emergency management, in addition to many other areas [21]. As you can understand, Wireless sensor networks are highly prone to faults and errors due to their restrictive capabilities and limited resources [22]. These environments have demanding security requirements that must be addressed in an attempt to focus on a spherical security strategy that will cover as many problems as possible such as security, routing, computing capability, and battery power. There are important factors, shown in figure 3, should be considered while designing a protocol or an algorithm for sensor networks such as dynamic topology, power consumption, fault tolerance, scalability, security, and WSN to the Internet connectivity. In addition, these influencing factors can be used to compare different schemes [4].
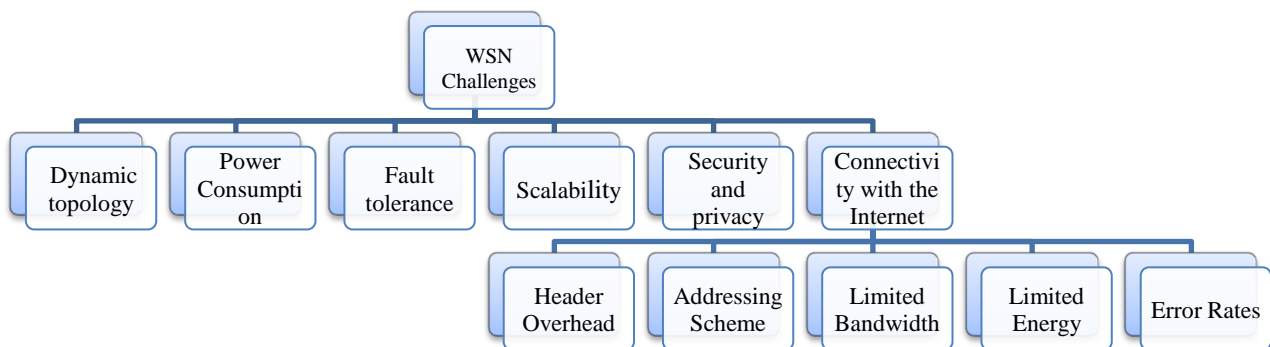

Figure 3: Wireless sensor Networks Challenges

4.1. Dynamic topology:
In most WSN applications it is assumed that the SNs are stationary. This means that SNs can determine the optimal paths among SNs [4]. However, in reality, it is not due to the fact that hundreds to several thousands of nodes are densely deployed all over the sensor field and the network topology changes time and again [23,24]. One of the most important obstacles facing the use of WSN is the topology management. The overhead increases because of the dynamic topology, which in essence leads to power consumption. One solution to maintain power consumption is to allow SN to sleep periodically when it's not in use. The essential concept of topology management is the ability to preserve a fully connected network at all times during the lifetime of the WSN [25].

4.2. Power consumption:
Transceiver is the significant energy consumer component in a sensor node because the communication process consumes more energy compared to data processing [26]. The most commonly used energy storage component in sensor node is the battery. A battery can be rechargeable or non-rechargeable. A sensor node is energy constrained due to the limited power of a battery and the difficult maintenance of it. Since WSNs are application specific networks, thus the functional lifetime of sensor network may be of months to years [27], this means that a battery will need a replacement every few days, which is unsuitable for most of the real time applications.

Energy saving and load balancing must be taken into account in the design and applications of WSNs and the implemented protocols [12]. One solution to the energy problems may be energy harvesting or energy scavenging, which means that SN is capable for extracting energy from ambient sources [4].

4.3 Fault tolerance:
The fault tolerance of a sensor network is the ability to sustain its functional capability stable without any intermission due to any sensor node failures [28]. The failure of sensor nodes may be due to lack of power, physical damage, or environmental interference. Each individual sensor node can be easily captured by malicious attacks [29]. The failure of SNs should not affect the sensor network processes. This is the reliability or fault tolerance issue. The fault tolerance level is a variant and depends on the

application of the sensor networks hence; the WSNs schemes must be developed with this in mind. In order to guarantee the network quality of service it is essential for the sensor network to be able to detect and heal failures.

4.4. Scalability:
The number of nodes in sensor networks, as well as the density of deployment, can be orders of magnitude higher than in ad hoc networks this of course involves thinking about scalability issues [30]. The density can range from few to hundreds sensor nodes in a region, which can be less than 10 m in diameter [31]. From the other points of view, the number may reach an extreme value of millions. The new schemes must be able to work with this number of nodes [11]. The large number of nodes heavily impacts simulation performance and scalability and the credible results demand an accurate characterization of the sensor radio channel [32]. New aspects must be included in simulators leading to different degrees of accuracy versus performance.

4.5. Security and privacy:
Since the SN's computational capacity, memory and available power are limited, reliable data transfer becomes challenging in the wireless environment. The sensors are deployed either in a controlled environment or in an uncontrolled environment where security for sensor networks becomes extremely important [33]. As the transfer of data is on wireless channel the privacy and security is an important concern of these networks. For the right data transfer, there should be a special care for malicious attacks and noisy wireless channel. WSN are sensitive to various attacks such as Denial of Service (DoS), Wormhole attack, Hello flood Attack, Sinkhole Attacks, Sybil Attack etc. [34, 35]. These attacks can be attended by various strategies depending on service types, data type and computational capacity of the nodes.

4.6. Connectivity:
There are a number of reasons why IP cannot be used directly at the sensor level, reserving the routing for dedicated protocols [36]. To solve this problem efficiently is not an easy task, as in WSN SNs are realized with many limited resources. Many features should be satisfied for efficient WSN-Internet interworking having a great impact on connections such as header overhead, addressing scheme, limited bandwidth, limited energy, error rates. Also, some potential solutions will be described in the next section.

- **Header Overhead:** IPv4 currently still manages to satisfy the great majority of computer communication needed across the Internet, mainly due to several methods like network address translation (NAT). The IP addresses are running out. One solution is to use the IPv6. However, The IPv6 protocol will result in complication in the expected overhead of IP for WSN. For example, the IPv6 header consumes 40 bytes without any additional extension headers. In contrast, the media access control layer (MAC) has a maximum frame size of 102 octets [37], leaving just 62 bytes for every single IPv6 packet. Thereby, no link layer encryption or IPv6 extension headers are taken into account.

In addition, IP adds important amount of data on the header block of the packet, leading to undesirable overhead. For example, for small messages a four-byte data message would have a header overhead of approximately 90% [4]. A lot of

energy is spent on communication and data transmission this will be a very

obstructive factor for the use of IP on the smart SN. The header size increases and power spent increases as well. One way to overcome this problem is using header compression techniques, applying mechanisms to the addresses (by using link-local addresses for instance) [38] or even applying the compression mechanisms defined by the 6LoWPAN specification.

- **Addressing Scheme:** IP addressing method depends on the understanding of the sender and the receiver addresses, and it must be unique within the same network. In ordinary IP networks, address assignment is done either using manual configuration done by administrator or a dynamic mechanism such as Dynamic host configuration protocol (DHCP). In a large -scale sensor network, manual configuration is not possible and dynamic methods are usually expensive in terms of communication. In case of sensor networks, mobility management is required especially for sensor networks in the deployment of IPv6, providing a huge address space suitable to address large sensor networks globally with a built-in auto configuration and supporting network mobility (NEMO) [38]. One way to overcome this problem is proposing a spatial IP address assignment scheme that provides semi- unique IP addresses to sensor nodes [39].

- **Limited Bandwidth:** Many new WSN applications are constantly rising and much more applications will appear moving forward to the future. Numerous Internet hosts try to get information from WSNs so the interworking architecture should be suitable for a large number of sensor nodes and Internet hosts [5]. Therefore, the Interworking architecture should be designed in an expandable manner. However, Small sensors have limited wireless bandwidth hence, the data transmission will take longer time. With limited bandwidth one does not want to waste bits on overhead, even if it is for header, error control, or others to overcome the header overhead problem. Hence, header compression techniques can be used.

- **Limited energy:** Energy is considered as a scarce resource for a sensor node, especially when a node is deployed with a battery in a remote region. Once the SN consumes all the amount of the available energy, it is almost impossible to provide substitute energy [40]. Therefore, a balanced energy management between the supply and the load is required in order to avoid energy deficiency in a network to increase the lifetime sensor node. Wireless network communications on the nodes consume the enormous amount of energy, involving both transmitting and receiving of data. In certain circumstances the energy cost of 1 bit transmission corresponds to 1000 processor instructions or more [3].

In many states it is not viable to provide battery charging or battery replacement. Thus, when a sensor node loses its power it dies. Moreover, the header overhead, limited bandwidth and addressing techniques may result in power consumption.

Dividing the sensor network into small clusters would be an efficient solution to solve the problem of energy consumption. Another solution would be the use of energy harvesting nodes, which collect energy from environment leaving the SN as alive as possible.

- **Error Rates:** The TCP/IP protocol suite is developed for networks with very low error rates and unfortunately it does not work well in WSN, which is an error prone environment. Hence, a mechanism that lets SNs help each other in collecting data segments is a must. The design of the framework must satisfy the reliability feature.

- One solution is distributed TCP caching when the segments are lost because of any type of errors; neighboring SNs are able to re-transmit the lost segments.

It is important to understand the constrained capabilities of sensor nodes if you wish to develop a proper security solution against known malicious attacks. Table 2 concludes the most important research directions of WSN challenges.

Table 2: Recent Research Directions In WSN

Limitations	Approaches	Objectives	Future directions
Network topology	Particle swarm optimization based clustering algorithm with mobile sink [41].	Improving network performance by combining The virtual clustering technique with the PSO algorithm.	Improving the algorithm to be more efficient.
	Novel constrained iterative average path length reduction algorithm [42].	Using two different frequency bands. The first band is used for creating conventional links and the second band for link addition in an iterative manner for maintaining the small world characteristics of the network.	Development of localization methods that are designed to utilize the power of small world WSN in the context of data aggregation and node fault detection.
	Toward Source Tree novel algorithm [43].	Generating approximate Steiner Trees in wireless sensor networks.	Developing an algorithm, which optimizes other metrics jointly such as the throughput, load balancing, and congestion control.
Power Consumption	K-coverage model of mobile WSNs [44].	Searching for the optimal sensor covers which extend the network lifetime.	To measure its performance in additional environments such as the environment with sensors heterogeneity.
	Community-Based Routing with Ant Colony Optimization protocol (CB-RACO) [45].	Reducing the cost of the agent's tour, mostly in terms of distance and the energy consumed, provided by the intra-community routing strategy.	Improving CB-RACO in order to support data gathering with multiple mobile Sinks as well as to estimate the overall network lifetime and load balancing in such scenarios.
Fault Tolerance	Heterogeneous fault diagnosis protocol [46].	Detecting and correcting such environmental heterogeneous faults.	Implementing and validating the algorithm on real sensor network hardware.
	Adaptive Virtual Relaying Set (AVRS) [47].	A set of relay nodes with more reliable connections to the sender node is selected to form its Virtual Relaying Set (VRS) to help transmit packets.	Developing and describing a more efficient version of this approach.
Scalability	Blind-zone centroid-based scheme (BCBS) [48].	Healing the coverage holes efficiently by maximizing the coverage with the evenest distribution.	Developing this scheme to be more efficient.
	Disturbed centroid-based scheme (DCBS) [48].	Healing the coverage holes efficiently with higher coverage in a shorter time and moderate in the deployment time, moving distance and uniformity.	Developing this scheme to be more efficient.

	Limitations	Approaches	Objectives	Future directions
Security &Privacy		Efficient dynamic authentication and key Management scheme for heterogeneous WSN [39].	Providing a single lightweight protocol for both authentication and key establishment while optimizing the security level.	Extending protocol to address other security issues including data integrity and freshness.
		An efficient privacy-preserving compressive data-gathering scheme [49].	Proposing scheme offers two significant privacy-preserving features, packet flow intractability and message content confidentiality, which can efficiently thwart traffic analysis/flow tracing attacks.	Improving mechanism to increase security over large areas.
		Sensor network encryption protocol. SNEP [50].	Achieving semantic security, which prevents eavesdroppers from inferring the message content from the encrypted message.	Improving the protocol to be more efficient.
Connectivity with the Internet	**Header Overhead**	Dynamic Energy-aware Tree base Node Addressing (DEATBNA) [51].	Minimizes routing and addressing overhead. Energy based tree will result in a prolonged lifetime of the network.	Implementation of the proposed algorithm and comparing results with a set of existing routing algorithms.
	Addressing Scheme	Optimal addressing-based routing scheme for 6LoWPAN [52].	Proposes an address update algorithm and the descendants of a failed node can use this algorithm to update their addresses rather than reacquire the new addresses.	Taking advantage of AR's computing capabilities and storage resources to exploit its potential for assisting routing for 6LoWPAN.
	Limited Bandwidth	Extensible and flexible architecture for Integrating Wireless Sensor Networks with the Cloud [53]	Used REST-based Web services as an interoperable application layer that can be directly integrated into other application domains for remote monitoring.	Integrating Body Sensor Networks (BSNs) to the Cloud for real-time patient monitoring and notification.
	Limited Energy	Dynamic Energy-aware Tree base Node Addressing (DEATBNA) [51].	Minimizes routing and addressing overhead. Energy based tree will result in a prolonged lifetime of the network.	Implementation of the proposed algorithm and comparing results with a set of existing routing algorithms.
	Error Rates	Multi-objective adaptive swarm optimization (MASO) method for clustering [54].	Error rates optimization and improvement of the network lifetime in the wireless sensor network where clustering technique is used.	Working for a large network and trying to optimize work more accurately for inter-cluster communication.

5. CONNECTING WIRELESS SENSOR NETWORKS TO THE INTERNET.

Most of the WSN applications aim at watching the external/internal phenomenon. Few examples of these are Building environment monitoring, wild- Life Habitat Monitoring, Forest fire-detection etc. For such kind of applications, the sensor networks cannot function in complete isolation. There must be a way to gain access to the data produced by the sensor network, which can be done by connecting the sensor network to existing network infrastructure such as the Internet [53]. Main design challenges concerning the interconnection between the Internet and WSNs must provide: a) access to each SN through the TCP/IP based network; b) efficient communications from the aspect of SN's energy consumption; and c) transparency in operation between TCP/IP based protocols and WSN protocols [4].
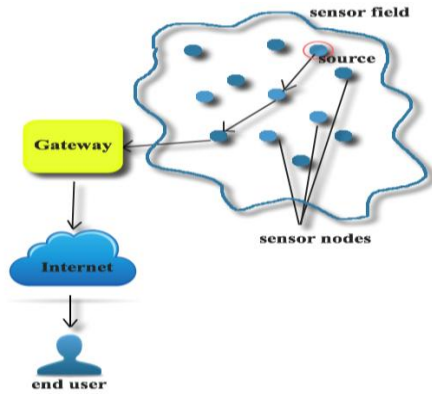
Figure 4: Connecting sensor field to the Internet through a Gateway

There are several integration approaches to connect WSN to the Internet. Each approach tries to consider these challenges and overcome them to achieve the best compromise among the WSN constraints and the standardization of TCP/IP protocols [56]. So far, several studies have been conducted for WSN-Internet interworking [57,58,59,60]. These works can be divided into two categories: gateway-based and overlay-based approaches shown in figure 5.
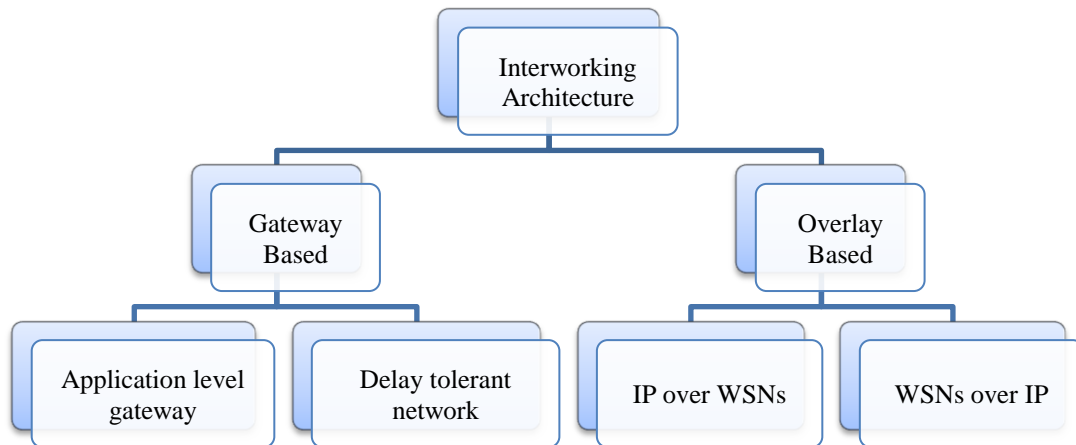

Figure 5: WSN to the Internet interworking Architecture

5.1. Gateway-based Approach

A gateway is an essential element to connect a WSN with the Internet, which performs several tasks such as protocol conversion and message relay [56]. A simple gateway-based approach is to use an application layer gateway as shown in figure 3a. The application layer gateway receives query messages from the Internet and translates it into a new one that can be interpreted on the WSN all interworking processes are performed only at the application layer gateway hence the application layer gateway is designed only for a specific application, Therefore, it does not incur high initial deployment costs. WSNs and the Internet are fully separated so that optimized protocols for each network can be individually applied. However, the gateway can be a single point of failure. One solution is to deploy multiple gateways. Other issues such as synchronization between gateways and load distribution can be raised in this case [56]. In addition, since the application layer gateway is designed for a specific application, it is not extensible.

Another gateway-based approach is to use a delay tolerant network (DTN) gateway [61]. The DTN architecture implements one new layer, both in TCP/IP and WSN networks as shown in figure 3b, referred as Bundle Layer which takes care of delivering messages from other regions to hosts within the local region by storing and forwarding packets between two networks. The DTN design contains numerous principles to provide service to support interoperability of heterogeneous regions as mentioned in [61]. The DTN is a new network designed to address several challenging issues, e.g., long and variable delay, asymmetric

data rates, and high error rates [60]. In the DTN architecture, when the DTN gateway receives a packet from the Internet, the DTN gateway transforms the lower layer messages of the bundle layer into those of WSNs and then delivers it to WSNs. In case the link of WSNs is broken due to the high error rate, the packet is not forwarded and stored for future forwarding. Different from the application layer gateway approach, the DTN gateway can be used for various types of applications and thus the DTN gateway-based approach provides higher extensibility [65].
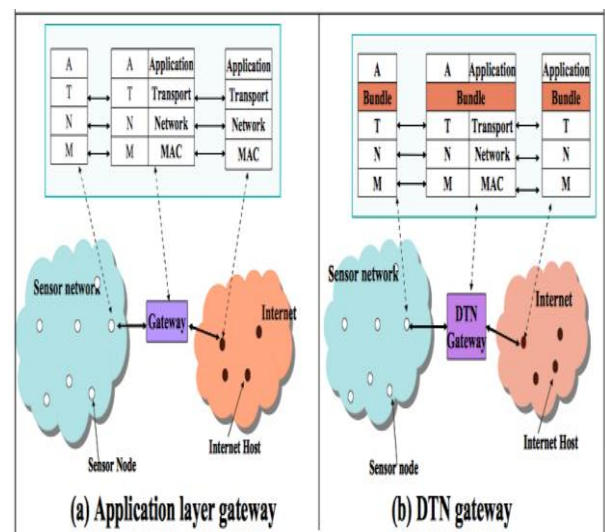

Figure 6: Gateway-based Approach [56].

5.2.Overlay-based Approach

Directly employing the TCP/IP protocol suite as the communication protocol in the sensor network would enable seamless integration of the sensor network and any TCP/IP network [58]. No special midway nodes or gateways would be needed for connecting a sensor network with a TCP/IP network. TCP/IP in the sensor network would also provide the possibility to route data to and from the sensor network over standard technologies such as General Packet Radio Service (GPRS) [62].

The first overlay-based approach is to implement an IP overlay network over WSNs [61] Sensor nodes need to be equipped with IP protocol stacks for addressing and routing but it is quite difficult to assign IP addresses to all sensor nodes. Therefore, only a few nodes, e.g., cluster heads, configure their IP addresses and constitute an IP overlay network among cluster heads as shown in figure 4a. As known, the Internet uses address-centric protocols and WSN uses data-centric protocols. A key issue of this approach is how to interwork both networks despite the differences between routing protocols concept. One solution to this problem is establishing a tunnel between cluster heads and a data-centric routing protocol can be implemented over this tunnel [56]. The main advantage of this approach is that it does not need any flooding of messages and an Internet host can directly send message to IP- addressable nodes.

The second approach is to construct an overlay WSN over the Internet [59]. When the packets are transmitted from WSNs arrive at the gateway, they are encapsulated within a typical TCP/IP packet and then delivered to a specific Internet host. In an overlay WSNs over the Internet, the major components are virtual nodes running over the Internet and overlay gateways. A virtual node is an Internet host that operates a WSN protocol stack over the TCP/IP protocol stack forming a virtual sensor network over the Internet [56]. The overlay gateway has two protocol stacks for the Internet and WSNs. It

performs the packet transformation in a way more simple than the gateway-based approaches because it encapsulates the received packet into a typical TCP/IP packet, without any interpretation at the gateway level shown in figure 4b. Since virtual sensor nodes handle both the TCP/IP and sensor network protocol stack, a high overhead may be incurred. On the other hand, virtual sensor nodes can be implemented by software, so that it has an advantage of easy deployment.
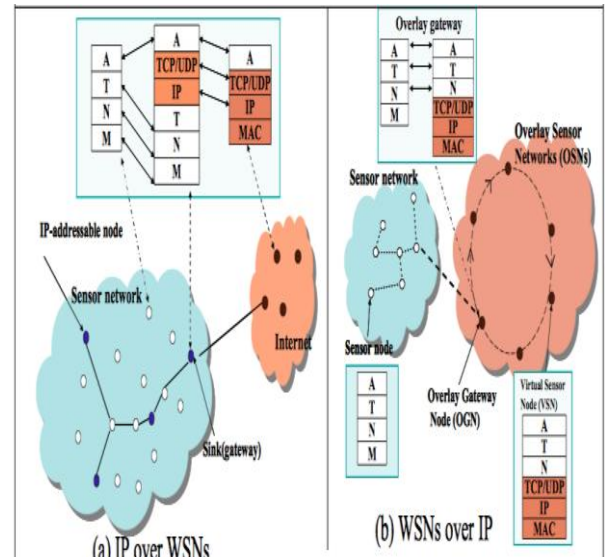

Figure 7: Overlay Based Approach [56].

Having all this in mind, it's obvious that for Homogeneous Wireless Sensor Networks the application level gateway approach is more suitable conversely for the Heterogeneous Wireless Sensor Networks, the IP overlay network over WSNs approach would be better. Table 3 shows the main advantages and drawbacks of each approach and the recommended solution.

Table 3: WSN to the Internet Interworking Architectures

	Approach	Concept	Advantages	Drawbacks	Recommended solutions
Gateway approaches	**App. Level gateway**	The application layer gateway receives query messages from the Internet and translates it into a new one that can be interpreted on the WSN all interworking processes are performed only at the application layer gateway.	Simple to apply since WSNs and the Internet are fully separated so that optimized protocols for each network can be individually applied.	A single point of failure.	Deploying multiple gateways taking into account issues such as synchronization between gateways and load distribution.
				Designed for a specific application, it is not extensible.	The DTN architecture.
	DTN gateway	Implements one new layer, both in TCP/IP and WSN networks referred as Bundle Layer which takes care of delivering messages from other regions to hosts within the local region.	Address several challenging issues, e.g., long and variable delay, asymmetric data rates, and high error rates. Provides higher extensibility.	Extra bundle layer that needs to be installed.	Header compression techniques
Overlay-based Approaches	**IP Overlay over WSNs**	Few nodes e.g., cluster heads, configure their IP addresses and constitute an IP overlay network among cluster heads.	Does not need any flooding of messages and an Internet host can directly send massage to IP- addressable nodes.	Interworking both networks despite the differences between routing protocols concept.	Establishing a tunnel between cluster heads and a data-centric routing protocol can be implemented over this tunnel.

	WSN overlay over the Internet	Virtual nodes running over the Internet and overlay gateways operating a WSN protocol stack over the TCP/IP protocol stack forming a virtual sensor network over the Internet.	Performs the packet transformation in a way more simple than the gateway-based approaches. Easy deployment since virtual sensor nodes can be implemented by software.	High overhead may be incurred.	Header compression techniques.

6. EXISTING INTERWORKING APPROACHES:

As mentioned before, WSNs have already achieved success in many applications such as environmental monitoring, commercial application, industrial management, military and many more. Thus, WSNs applications need to be integrated with the IoT. Many approaches have been proposed to connect the two networks. Table 4, discuss the existing interworking approaches and their future work

Table 4: Existing WSN to the Internet Interworking approaches

Approach	Objective	Performance Metrics	Future work
A Web Services approach for the design of sensor networks, in which sensor nodes are service providers and applications are clients of such services [63].	Enabling a flexible architecture where sensor networks data can be accessed by users spread all over the world. Also, to provide the underpinning for building more general purpose networks, instead of strictly task-specific ones, in order to assist a large range of users, possibly spread over the world,	• Energy cost • Data transmission delay	Providing an ubiquitous, standardized access through a common and application independent interface.
The integration of WSNs sensing capabilities in the IMS [64]. **This solution is based on an extension of the 3GPP presence architecture.**	Enabling the distribution of end-user presence information (e.g. location, availability), a subset of context information, to interested parties, generally applications.	• Availability • Localization	Investigating the remaining issues related to WSNs/IMS integration, namely: information modeling and processing, the discovery of WSN gateways by the PS, and the definition of the outbound interfaces' related protocols and interactions. Also, working on a generic WSN/IMS gateway solution.
Sensor Networks for an All-IP World (SNAIL) approach to the IOT [65]. **The proposed architecture includes a complete IP adaptation method.**	Making a pivotal contribution to the realization of the IoT through the building of a suitable network of things. One of the important steps toward reaching this objective is to facilitate feasible IP-WSN technologies that incorporate into a complete architecture.	• UDP Round Trip Time • ICMPv6 round trip time • Hop count • End-to-end delay	Involving network management, service discovery, and a quality-of-service-aware routing protocol, as well as optimization of the proposed protocols. Investigating how the things network can be integrated into the IoT architecture will be another significant step to take.
A Framework for Integrating WSNs and External Environments [66].	Creating a generic framework that is able to adapt with the multitude of applications running on sensor nodes and exposes WSNs as a set of web services to external environments.	• Availability • Transmission delay. • Localization	Investigating and designing a more stable method for estimating the ranging and location based on RSSI value.
All-IP wireless sensor networks for real-time patient monitoring [67].	Reducing the communication delay so that, a physician can get any patient's physical parameters at any time and at many places.	• Communication delay • Control cost • Packet loss rate	Improving the model to be more efficient.

6.1 Performance Metrics:

Measuring performance is key to evaluating how well developers are doing their work and meeting their targets. Every developer uses different metrics according to their work to evaluate network performance. In [63], the authors checked the energy cost and transmission delay enhancement. In [64], the authors used availability and localization as performance metrics. In [65], they observed the data transmission delay and hop count to evaluate their model performance. In [66], they regarded the availability, transmission delay, and localization. In [67], the authors viewed the communication delay and packet loss rate to estimate their model. Table 5 summarizes the performance metrics used in each approach.

Table 5: Performance metrics used in these Approaches

Approach	Transmission Delay	Energy Cost	Availability	Localization	Hop count	Packet loss
[63]	√	√				
[64]			√	√		
[65]	√				√	
[66]	√		√	√		
[67]	√					√

7. CONCLUSION

WSN is one of the important distributed applications that recently appeared in several areas. However, the specificity of their architecture deployed in many IT industries makes it prone to a large number of issues such as dynamic topology, power consumption, fault tolerance, connectivity, and security. This paper focused on the connectivity issues between WSN and the Internet generally. The WSNs concept and most important applications were highlighted. In addition, this paper reviewed the WSN to the Internet Interworking different approaches such as gateway-based approach and relay-based approach pointing the advantages and drawbacks of each. The paper stated the most important challenges should be satisfied with efficient WSN-Internet interworking such as header overhead, addressing scheme, limited bandwidth, limited energy, error rates and described some potential solutions. Along with the current research projects, more development in solutions to the open research issues as described in this paper is motivated.

Finally, The interconnection between WSN and the Internet would come with several challenges and problems and it's not feasible to implement a full IP stack on sensor networks. Thus, the future direction is to focus on the problem of connectivity. Multiple gateways as a solution connecting heterogeneous WSNs in real time will be considered using Link cost method to select a gateway taking into account the enhancement of network lifetime, throughput and power consumption as well.

8. REFERENCES

[1] Prof. Madhav Bokare, Mrs. Anagha Ralegaonkar, "Wireless Sensor Network: A Promising Approach for Distributed Sensing Tasks", Excel Journal of Engineering Technology and Management Science, January 2012, Volume I - No.1, pp. 1-9.

[2] Shu Yinbiao, Kang Lee, Peter Lanctot , "Internet of Things: Wireless Sensor Networks", International Electrotechnical Commission, 2014.

[3] Renuka Roselin Kujur, A.K. Dwivedi, "Exploration of Existing Frameworks for Connecting Wireless Sensor Networks (WSNs) with Current Internet", International Journal of Computer Applications, January 2014, Volume 86-No 4, pp. 14-17.

[4] Mirko R. Kosanović, Mile K. Stojčev, "Connecting Wireless Sensor Networks to Internet", FACTA UNIVERSITATIS Series: Mechanical Engineering, 2011, Volume 9-No 2, pp. 169 - 182.

[5] Min Zhang, Sangheon Pack, Kideok Cho, Dukhyun Chang, Yanghee Choi, and Taekyoung Kwon, "An Extensible Interworking Architecture (EIA) for Wireless Sensor Networks and Internet", in Proc. Asia-Pacific Network Operations and Management Symposium (APNOMS) 2006 Poster Sessions, Busan, Korea, September 2006.

[6] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", ACM/IEEE International Conference on Mobile Computing and Networks (MobiCom 2000), Boston, Massachusetts, August 2000.

[7] Hakima Chaouchi, Jean-Marie Bonnin, "Wireless sensor networks: A survey on recent developments and potential synergies", The Journal of Supercomputing, April 2013, Volume 68 – No 1, pp. 1–48.

[8] S. Chen, Y. Wang, X.Y. Li, X. Shi, "Data Collection Capacity of Random-Deployed Wireless Sensor Networks", Proc. IEEE GLOBECOM, December 2009, pp. 1-6.

[9] Ibrahiem M.M.El Emery, S.Ramakrishna, "Wireless Sensor Networks: From Theory to Applications", CRC Press, Taylor & Francis Group, 2013.

[10] D. Estrin, R. Govindan, J. Heidemann, S. Kumar, "Next century challenges: Scalable coordination in sensor networks", Proc. 5th Annual ACM Int. Confe. Mobile Computing Networking MobiCom'99, Washington, USA, August 1999, pp. 263–270.

[11] Magdi S. Mahmoud, Yuanqing Xia,"Networked Filtering and Fusion in Wireless Sensor Networks", CRC Press, New York, 2014.

[12] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey ", Computer Networks, 2001, Volume 38 - No 4, pp. 393-422.

[13] P. Bonnet, J. Gehrke, P. Seshadri, "Querying the physical world", IEEE Personal Communications, October 2000, Volume7 – No 5, pp. 10–15.

[14] A. Cerpa, J. Elson, M. Hamilton, J. Zhao, "Habitat monitoring: Application driver for wireless communications technology", Workshop on data communication in Latin America and the Caribbean, April 2001, Volume 31 – No 2, pp. 20-41.

[15] Savo Glisic, "Advanced Wireless Networks: Technology

and Business Models", Wiley, 2009, 2nd edn.

[16] Reis, Catarina I., Maximiano, Marisa da Silva, "Internet of Things and Advanced Application in Healthcare", IGI global disseminator of knowledge, United States, October 2016.

[17] B. Sibbald, "Use computerized systems to cut adverse drug events: report", CMAJ: Canadian Medical Association Journal, June 2001, Volume 164 No.13, pp. 1878-1878.

[18] E.M. Petriu, N.D. Georganas, D.C. Petriu, D. Makrakis, V.Z. Groza, "Sensor-based information appliances", IEEE Instrumentation and Measurement Magazine, December 2000, Volume 3 – No 4, pp. 31–35.

[19] Ian F. Akyildiz, Mehmet Can Vuran, " Wireless Sensor Networks", John Wiley & Sons Publications, 2010.

[20] Ashwini R., Pooja Mohnani, "Application of Wireless Sensor Network in Home Automation", International Journal of Computer & Organization Trends, June 2014, Volume 4- No 3.

[21] Darwish A, Hassanien AE, "Wearable and Implantable wireless sensor network solutions for healthcare monitoring", Sensors, 2011, Volume 11- No 6, pp. 5561-5595.

[22] Heshem A. El Zouka, "Challenges in Securing Wireless Sensor Networks", The Seventh International Conference on Sensor Technologies and Applications, Barcelona, Spain, 2013.

[23] C. Intanagonwiwat, R. Govindan, D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks", Proceedings of the 6th annual international conference on Mobile computing and networking, Boston, MA, 2000, pp. 56–67.

[24] J. A. Stankovic, T. F. Abdelzaher, C. Lu, Lui Sha, and J. C. Hou, "Real-time communication and coordination in embedded sensor networks", in Proceedings of the IEEE, July 2003, Volume 01 - No. 7, pp. 1002-1022.

[25] Lisa Frye, Liang Cheng, Shenfu Du, Michael W. Bigrigg, "Topology Maintenance of Wireless Sensor Networks in Node Failure-prone Environments", IEEE International Conference on Networking, Sensing and Control, FL, USA, 2006.

[26] C. Schurghers, V. Raghunathan, S. Park, M. Srivastava, "Energy-Aware Wireless Microsensor Networks", IEEE Signal Proc Mag., 2002, Volume 19- No2, pp. 40–50.

[27] Sidra Aslam, Farrah Farooq, Shahzad Sarwar, "Power Consumption in Wireless Sensor Networks", Proceedings of the 7th International Conference on Frontiers of Information Technology, Pakistan, December 2009.

[28] G. Hoblos, M. Staroswiecki, A. Aitouche, "Optimal design of fault-tolerant sensor networks", IEEE International Conference on Control Applications, Anchorage, USA, September 2000, pp. 467–472.

[29] Ruiping Ma, Liudong Xing, Howard E. Michel, "Fault-Intrusion Tolerant Techniques in Wireless Sensor Networks", 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, USA, December 2006.

[30] Javier Gomez, J. Antonio Garcia-Macias, "MANET and WSN: Are they alike?", International Conference on Parallel Processing Workshop 2005, 2006, pp. 1-20.

[31] S. Cho, A. Chandrakasan, "Energy-efficient protocols for low duty cycle wireless microsensor", Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, 2000.

[32] E. Egea-Lopez, J. Vales-Alonso, A. S. Martinez-Sala, P. Pavon-Mariño, J. Garcia-Haro, "Simulation Scalability Issues in Wireless Sensor Networks", IEEE Communications Magazine, July 2006, Volume 44- No 7, pp. 64-73.

[33] Anjali Potnis, and C S Rajeshwari, "Wireless Sensor Network: Challenges, Issues, and Research", Proceedings of 2015 International Conference on Future Computational Technologies, Singapore, March 2015, pp. 224-228.

[34] Y. Wang, G. Attebury, Byrav Ramamurthy, "A survey of security issues in wireless sensor networks", IEEE Communications Surveys & Tutorials, 2006, Volume 8-No 2, pp. 2-23.

[35] Mayur Dhaye, Himangi Pande, "Security in Wireless Sensor Networks: issues and Challenges", 8th International Conference Advanced Communication Technology, Phoenix Park, South Korea, February 2006.

[36] Paulo Alexander, "Internet protocol over wireless sensor networks, from myth to reality", Journal of communication, March 2010, Volume 5 - No 3, pp. 189-196.

[37] G. Montenegro, N. Kushalnagar, " Transmission of IPv6 Packets over IEEE 802.15.4 Networks ", RFC 4944, September 2007.

[38] Karl Mayer, Wolfgang Fritsche, "IP-enabled Wireless Sensor Networks and their integration into the Internet", Proceedings of the First International Conference on Integrated Internet Ad hoc and Sensor Networks, France, May 2006.

[39] S.Athmani, A.Bilami, D. E .Boubiche, "An efficient dynamic authentication and key management mechanism for heterogeneous WSNs", Future Generation Computer Systems, November 2017.

[40] I. Talzi, A. Hasler, S. Gruber, C. Tschudin, Permasense, "investigating permafrost with a wsn in the swiss alps", Proceedings of the 4th workshop on Embedded networked sensors, 2007, pp. 8–12.

[41] Jin Wang, Yiquan Cao, Bin Li, Hye-jin Kim, Sungyoung Lee, "Particle Swarm Optimization based Clustering Algorithm with Mobile Sink for WSNs", Future Generation Computer Systems, November 2017, Volume 76, pp. 452–457.

[42] Om Jee Pandey, Rajesh M.Hegde, "Node localization over small world WSNs using constrained average path length reduction", Ad Hoc Networks, December 2017, Volume 67- No C, pp. 87–102.

[43] Hongyu Gong, Luoyi Fu, Xinzhe Fu, Lutian Zhao, Kainan Wang, and Xinbing Wang, "Distributed Multicast Tree Construction in Wireless Sensor Networks", IEEE Transactions on Information Theory, January 2017, Volume 63- No 1, pp. 280-296.

[44] Mohamed Elhosenya, Alaa Tharwatb, Xiaohui Yuanc, Aboul Ella Hassaniend, "Optimizing K-coverage of mobile WSNs", Expert Systems With Applications, February 2018, Volume 92, pp. 142-153.

[45] Valerio Rosseta, Matheus A. Pauloa, Juliana G. Cespedesa, Maria C. V. Nascimentoa, "Enhancing the Reliability on Data Delivery and Energy Efficiency by Combining Swarm Intelligence and Community Detection in Large-scale WSNs", Expert Systems with Applications, July 2017, Volume 78, pp. 89-102.

[46] Rakesh Ranjan Swain, Pabitra Mohan Khilar, Sourav Kumar Bhoi, "Heterogeneous Fault Diagnosis for Wireless Sensor Networks", Ad Hoc Networks, February 2018, Volume 69, pp.15-37.

[47] Anfeng Liua, Zhuangbin Chena, Neal N.Xionga, "An Adaptive Virtual Relaying Set Scheme for Loss-and-Delay Sensitive WSNs", Information Sciences, January 2018, Volume 424, pp.118–136.

[48] Wei Fang, Xinhong Song, Xiaojun Wu, Jun Sun, Mengqi Hu, "Novel Efficient Deployment Schemes for Sensor Coverage in Mobile Wireless Sensor Networks", Information Fusion, May 2018, Volume 41, pp. 25-36.

[49] Kun Xiea, Xueping Ninga, Xin Wangb, Shiming Hec, Zuoting Ninga, Xiaoxiao Liud, Jigang Wene, Zheng Qina, "An efficient privacy-preserving compressive data gathering scheme in WSNs", Information Sciences, June 2017, Volume 390, pp. 82–94.

[50] Chanchal Yadav, Raksha K, Supriya S. Hegde, Anjana N.C, Sandeep Kumar E, "Security Techniques in Wireless Sensor Networks: A Survey", International Journal of Advanced Research in Computer and Communication Engineering, April 2015, Volume 4-No. 4, pp. 289-295.

[51] Ganesh.S.Pise , Vinod. V. Kimbahune, "Energy Efficient Node Addressing Scheme in Hierarchical Wireless sensor Network", International Journal of Computer Science and Information Technologies, 2013, Volume 4-No 6, pp. 963-966.

[52] Xiaonan Wang, Qi Sun, Yuan Yang, Dong Wang, "Optimal addressing-based routing for 6LoWPAN", Computer Standards & Interfaces, March 2016, Volume 45- No C, pp. 79-89.

[53] Rajeev Piyare, Seong Ro Lee, "Towards Internet of things (iots): integration of wireless sensor network to cloud services for data collection and sharing", International Journal of Computer Networks & Communications, September 2013, Volume 5-No 5, pp. 59-72.

[54] Sharada KA, Dr.Siddaraju, "Error rate optimization and improved WSN lifetime", International Journal of Engineering and Innovative Technology, June 2016, Volume 5- No 12, pp. 55-58.

[55] Renuka Roselin Kujur, A.K. Dwivedi, "Exploration of Existing Frameworks for Connecting Wireless Sensor Networks (WSNs) with Current Internet", International Journal of Computer Applications, January 2014, Volume 86, No 4, pp.17-18.

[56] Karim Ahmed Awad El Sayed Emara, Prof. Dr. Taha El Areef, Prof. Dr. Mohammad Hashem, Dr. Mohammad Abdeen, "integrating wireless sensor networks with ip-based network", Masters Thesis, Department of Computer Science, Ain Shams University, Cairo, 2009.

[57] Z.Z. Marco, K. Bhaskar, "Integrating Future Large-scale Wireless Sensor Networks with Internet", USC Computer Science Technical Report CS 03-792, 2003.

[58] Dunkels, A., Alonso, J., Voigt, T., Ritter, H., and Schiller, "Connecting Wireless Sensornets with TCP/IP Networks", In Proceedings of the Second International Conference on Wired/Wireless Internet Communications, Berlin, Heidelberg, February 2004.

[59] H. Dai and R. Han, "Unifying Micro-Sensor Networks with the Internet via Overlay Networking", 29th Annual IEEE International Conference on Local Computer Networks, Tampa, FL, USA, November 2004.

[60] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets", Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, Karlsruhe, Germany, August 2003.

[61] Dunkels, A., Alonso, J., Voigt, T., Ritter, H., and Schiller, "Connecting Wireless Sensornets with TCP/IP Networks", In Proceedings of the Second International Conference on Wired/Wireless Internet Communications, Germany, February 2004.

[62] Cai, J., Goodman, D., "General packet radio service in GSM", IEEE Communications Magazine 35, 1997, pp. 122–131.

[63] Flávia Coimbra Delicato, Paulo F. Pires, Luci Pirmez, Luiz Fernando Rust da Costa Carmo "A Flexible Web Service based Architecture for Wireless Sensor Networks", Distributed Computing Systems Workshops, Rhode Island, USA, June 2003.

[64] May El Barachi, Arif Kadiwal, Roch Glitho, Ferhat Khendek, Rachida Dssouli, "A Presence-based Architecture for the Integration of the Sensing Capabilities of Wireless Sensor Networks in the IP Multimedia Subsystem", Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE, Las Vegas, NV, USA, April 2008.

[65] Sungmin hong, daeyoung kim, minkeun ha, sungho bae, sang jun park, woo- young jung, and jae-eon kim, "snail: an ip-based wireless sensor network approach to the internet of things", IEEE wireless communications, December 2010, Volume 17-No 6.

[66] Thanh-Dien Tran, Jorge SaSilva, "A Framework for Integrating WSNs and External Environments", IFAC Proceedings Volumes, 2010, Volume 43- No 17, P.p. 383-389.

[67] Xiaonan Wang, Deguang Le, Hongbin Cheng, Conghua Xie, "All-IP wireless sensor networks for real-time patient monitoring", Journal of Biomedical Informatics, December 2014, Volume 52, Pp. 406-417.