ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

Volume 11, Issue 3, May-June 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

IMPACT FACTOR: 7.583

| www.ijarasem.com | ijarasem@gmail.com | +91-9940572462 |

Opportunities and Challenges of Internet of Things (IoT) Integration with Wireless Sensor Networks

Dr. H K SHANKARANANDA

Principal, TMAES Polytechnic (Govt Aided), Hosapete, Karnataka, India

ABSTRACT: WSN can be used for terrestrial (TWSN) and underwater communication (UWSN). Underwater wireless sensor network has emerged as one of the important research areas for the conservation and exploitation of the ocean. Internet of Things (IoT) has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of radio-frequency identification (RFID), and wireless, mobile, and sensor devices. In an effort to understand the development of IoT in industries, this study reviews the current research of IoT, key enabling technologies, major IoT applications in industries, and identifies research trends and challenges. Commercial solutions can effectively address vertical application domains, but they often lead to technology lock-ins that limit horizontal composability and reuse. We review some important barriers that hinder WSN use in IoT applications and highlight the main effort and cost components. With these elements in mind, we propose an open hardware-software development platform that can optimize the value flow between technologies and actors with stakes in WSN applications. Wireless Sensor Node (WSN) is used to receive & transmit data and is often placed in remote areas. A wide range of industrial IoT applications have been developed and deployed in recent years.

KEYWORDS: Internet of Things (IoT), Wireless Sensor Node (WSN), pollution monitoring, oceanographic data collection, IoT applications.

I. INTRODUCTION

Wireless sensor network is a booming area for research and development. A sensor node in a network is capable of performing different operations like processing, gathering sensory information and communicating with other connected nodes in the network. Wireless sensor nodes are used for terrestrial and underwater applications. Terrestrial sensor nodes are used to monitor, detect and track various environmental phenomenon and events. The development of the miniature sized WSN with low power consumption facilitated TWSN to broaden their research to underwater techniques. UWSNs should be capable of establishing extraordinarily secure and efficient network links in harsh underwater environments. Underwater routing protocols must be flexible to manage complex topology modifications and maintain network reliability in the face of multiple emergencies. Routing protocols usually choose the route for transmitting information from underwater source nodes to surface destination nodes. Interest in UWSN has seen a steep rise among the research community. Researchers have published an impressive number of study and journals. Most papers focus on one property of the protocol, such as the node's energy consumption or geographical location. Most of the surveys lacked an efficient comparison of routing protocols. IoT has gained much importance due to the abundant usage of these tiny networked devices. These are smart, yet basic things that can sense and communicate wirelessly. WSN is a collection of sensor and routing nodes. which may be put together in the environment to predict physical conditions, such as wind, temperature, and many others. These networks collect and process data from tiny nodes and then transfer it to the operators. Besides WSN, IoT has also played an important role in human life. IoT and the digital age play essential roles in overcoming social and physical barriers and providing ease and mobility to people, resulting in improved and equal opportunities, and access to information.

II. LITERATURE REVIEW

Hamid Errachdi (2023) Marine environmental monitoring is increasingly vital due to climate change and the emerging Blue Economy. Advanced Information and Communication Technologies (ICTs) have been applied to develop marine monitoring systems, with the Internet of Things (IoT) playing a growing role. Wireless Sensor Networks (WSNs) are crucial for IoT implementation in the marine realm but face challenges like modeling, energy supply, and limited deployment compared to land-based applications.

Seokjoo Shin (2022) Underwater wireless sensor networks (UWSNs) are a prominent research topic in academia and industry, with many applications such as ocean, seismic, environmental, and seabed explorations. The main challenges in deploying UWSN are high ocean interference and noise, which results in longer propagation time, low bandwidth, and changes in network topology. To mitigate these problems, routing protocols have been identified as an efficient solution.

Mamoona Majid (2022) The 21st century has seen rapid changes in technology, industry, and social patterns. Most industries have moved towards automation, and human intervention has decreased, which has led to a revolution in industries, named the fourth industrial revolution (Industry 4.0). Industry 4.0 or the fourth industrial revolution (IR 4.0) relies heavily on the Internet of Things (IoT) and wireless sensor networks (WSN). IoT and WSN are used in various control systems, including environmental monitoring, home automation, and chemical/biological attack detection.

Rashmi M. Jogdand (2020) Internet of Things (IoT) is one of the emerging technologies comprises of ‘things’ capable of identifying, sensing, communicating, processing, and actuating the data gathered from the environment. IoT plays an important role in various sectors including healthcare, medical, education, smart cities, and also it contributes in developing smart industries as part of the industrial revolution ‘Industry 4.0’ with the use of Industrial Internet of Things (IIoT) technology.

Mohammad S. Obaidat (2020) The advanced technology Internet of Things (IoT), a recent development in wireless sensor networks, provides a way to connect surrounding physical objects to the Internet in a dynamic way. Major technology big giants Apple, Google, and Amazon's products are differentiated on the basis of measurement parameters such as their prices, streaming options, customisable appearance methods, major partnership companies related information appearing.

Internet of things

The Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. "Internet of things" has been considered a misnomer because devices do not need to be connected to the public internet; they only need to be connected to a network and be individually addressable. The field has evolved due to the convergence of multiple technologies, including ubiquitous computing, commodity sensors, and increasingly powerful embedded systems, as well as machine learning.

IoT security device

Internet of Things (IoT) security devices are electronic tools connected via Internet to a common network and are used to provide security measures. These devices can be controlled remotely through a mobile application, web-based interface or any proprietary installed software, and they often have capabilities such as remote video monitoring, intrusion detection, automatic alerts, and smart automation features.

Types of IoT Security Devices

1. **Surveillance Cameras:** These are one of the most common types of IoT security devices. They provide real-time video monitoring of the environment, allowing viewing footage remotely from the interface.
2. **Smart Locks:** Smart locks can be controlled remotely and can provide access to authorized individuals. Some also have features such as biometric recognition and automatic locking and unlocking based on proximity.
3. **Smart Alarms:** These devices can detect potential threats such as break-ins, fire, and carbon monoxide and send automatic alerts to homeowners, security units and, in some cases, local authorities.
4. **Door/Window Sensors:** These sensors trigger an alert when doors or windows are opened or tampered with.
5. **Smart Detectors:** These devices detect environmental hazards such as smoke, gas leaks, and water leaks, alerting in real time.

WSN programming models and tools

Early WSN implementations were manually coded close to hardware or the embedded operating system. Typically this brings smaller code size and higher execution efficiency at the cost of maintenance, portability and design reuse. It also requires a good understanding of various technologies underlying WSN nodes, which is difficult to find among software programmers and seldom found among application domain experts. Over time, as WSN cost, time to market and operation reliability increase in importance, higher programming abstractions and design automation techniques get increasing attention.

Evaluation of existing WSN programming models and tools

We will evaluate how the WSN development tools, tool categories and methodologies reviewed in can be used to reduce overall WSN application cost. We will also evaluate their potential to work in synergy with other tools in a comprehensive development platform that is suitable to cover the widening diversity of WSN applications and keep pace with the rapid technological evolution in the field.

Low-level programming evaluation
Low-level programming, be it OS- or VM-based, typically allows a good control over the node and good design optimization, but it often requires in-depth engineering and programming knowledge. This is rarely found among application domain experts and may also divert important design effort from application logic implementation. Embedded OSs and VMs have typically a layered structure which encapsulates well the hardware-dependent parts in order to facilitate their porting to other hardware nodes, which is important for keeping the pace with technology evolution.

WSN hardware and server-side support
In the following we will comparatively review some options for WSN node hardware and for server-side software.

Microcontroller
There are many families of low and very low power microcontrollers, each covering a broad range of capabilities such as storage size for programs (FLASH), data (RAM and EEPROM), and peripherals. Given the diverse and specialized offering, the design flow should assist the developer in selecting the optimal microcontroller for the application, since it can influence significantly node cost and energy consumption.
Microcontroller component package type and size has both a direct impact on the component cost and an indirect one on PCB cost through its size and number of pins. PCB size can further influence the size and cost of the sensor node package.

Semi-automated WSN HW/SW application synthesis
We will now discuss a semi automated hardware-software application synthesis flow to better understand its benefits in terms of the evaluation criteria presented at the end.
The flow can automatically select modules from a previously developed library to perform design composition, both hardware and software, in order to significantly increase the productivity of the developers through design reuse, and to allow fast design space exploration for application implementation optimization.

Synergies for WSN development tools and platforms
WSN platform development and update is a complex, interdisciplinary, and evolving task. As such, it benefits from allowing all interested parties bring their contribution to its development and extensive use. WSNs are at the center of a constantly increasing research interest, focused on various functional and technological issues. Research advances the state of the art and most promising results can be made available to many WSN industrial actors through WSN platforms. Reciprocally, the research community would benefit from a common, open, and free WSN platform available for experimentation. In exchange, the platform would gain from extensive testing, consolidation, porting to popular hardware, improved development tools, and extensions for innovative applications.

Wireless Sensor Network (WSN)
Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions. Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System. Base Station in a WSN System is connected through the Internet to share data. WSN can be used for processing, analysis, storage, and mining of the data.

Consumer and enterprise IoT applications
There are numerous real-world applications of the internet of things, ranging from consumer IoT and enterprise IoT to manufacturing and IoT. IoT applications span numerous verticals, including automotive, telecom and energy.
In the consumer segment, for example, smart homes that are equipped with smart thermostats, smart appliances and connected heating, lighting and electronic devices can be controlled remotely via computers and smartphones. Wearable devices with sensors and software can collect and analyze user data, sending messages to other technologies about the users with the aim of making users' lives easier and more comfortable. Smart buildings can, for instance, reduce energy costs using sensors that detect how many occupants are in a room. The temperature can adjust automatically -- for example, turning the air conditioner on if sensors detect a conference room is full or turning the heat down if everyone in the office has gone home.

Advantages of Wireless Sensor Networks (WSN)

Low cost: WSNs consist of small, low-cost sensors that are easy to deploy, making them a cost-effective solution for many applications.

Wireless communication: WSNs eliminate the need for wired connections, which can be costly and difficult to install. Wireless communication also enables flexible deployment and reconfiguration of the network.

Energy efficiency: WSNs use low-power devices and protocols to conserve energy, enabling long-term operation without the need for frequent battery replacements.

Scalability: WSNs can be scaled up or down easily by adding or removing sensors, making them suitable for a range of applications and environments.

Real-time monitoring: WSNs enable real-time monitoring of physical phenomena in the environment, providing timely information for decision making and control.

Important of IoT

IoT helps people live and work smarter. Consumers, for example, can use IoT-embedded devices -- such as cars, smart watches or thermostats -- to improve their lives. For example, when a person arrives home, their car could communicate with the garage to open the door; their thermostat could adjust to a preset temperature; and their lighting could be set to a lower intensity and color. In addition to offering smart devices to automate homes, IoT is essential to business. It provides organizations with a real-time look into how their systems really work, delivering insights into everything from the performance of machines to supply chain and logistics operations. IoT enables machines to complete tedious tasks without human intervention. Companies can automate processes, reduce labor costs, cut down on waste and improve service delivery. IoT helps make it less expensive to manufacture and deliver goods, and offers transparency into customer transactions. IoT is one of the most important technologies and it continues to advance as more businesses realize the potential of connected devices to keep them competitive.

The benefits of IoT to organizations

IoT offers several benefits to organizations. Some benefits are industry-specific and some are applicable across multiple industries. Common benefits for businesses include the following:

- Monitors overall business processes.
- Improves the customer experience.
- Saves time and money.
- Enhances employee productivity.
- Provides integration and adaptable business models.
- Enables better business decisions.
- Generates more revenue.

IoT encourages companies to rethink how they approach their businesses and gives them the tools to improve their business strategies.

Generally, IoT is most abundant in manufacturing, transportation and utility organizations that use sensors and other IoT devices; however, it also has use cases for organizations within the agriculture, infrastructure and home automation industries, leading some organizations toward digital transformation.

III. RESEARCH METHODOLOGY

A synergy of different research efforts in the field, mainly focused on the targeted topical area is needed. The main contribution and novelty of this review editorial is in line with that. IoT technologies in sustainable energy and environmental issues. IoT enabled Smart City. There were two options for the implementation of the proposed technique; using a hardware WSN test-bed or using a network simulator. The test-bed option requires multiple sensor nodes along with a gateway node which can be connected to internet. This option costs a lot .Therefore the work is implemented using a simulator. However, there are several network simulators for WSN. Each simulator has advantages and disadvantages and the most suitable was selected carefully. E-health Ambient assisted living systems. IoT technologies in Transportation and Low Carbon Products. This study editorial serves as an introduction to the Virtual Special Issue (VSI) of JCLEPRO devoted to the 4th International Conference on Smart and Sustainable Technologies, in Bol (Island of Brač) and Split, at the University of Split, (Croatia). The herein presented introductory review editorial was directed to the selected and accepted publications from the international conference SpliTech and published papers were divided into four main topical areas as already specified above. Overall were initially selected and invited for potential inclusion in the VSI SpliTech. After conducted peer-review process, based on the JCLP procedures, 29 of them were selected for inclusion in the VSI SpliTech 2019.

IV. RESULTS AND DISCUSSION

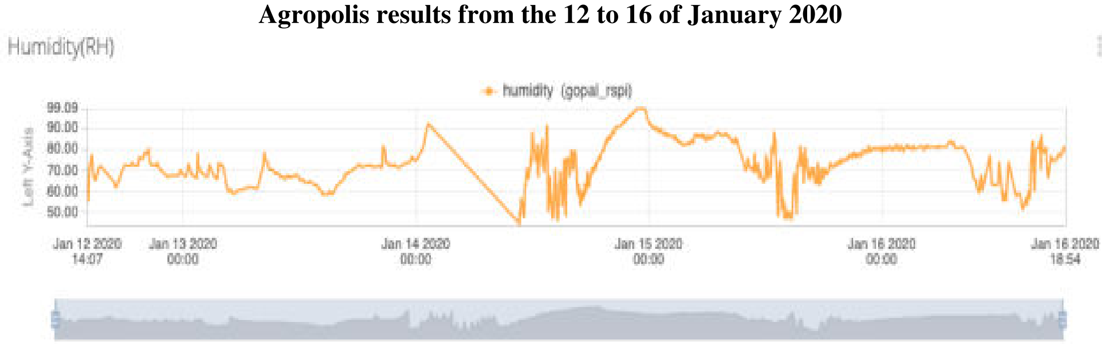
Threats become more attractive and dangerous as technology increases. Although new security mechanisms are being developed, intruders can easily find other ways to attack systems. Table 1 explains the network security attacks in the IoT and WSN domains. The attacks are categorized according to the open system interconnection (OSI) layered point of view.

Table 1: Network Security Attacks on IoT and WSN Layers.

Sr. No.	Layer Name	Attacks
1	Physical layer	Interception, radio interference, jamming, tempering, Sybil attack.
2	Data link layer	Replay attack, Spoofing, altering routing attack, Sybil Attack, collision, traffic analysis, and monitoring, exhaustion.
3	Network layer	Black hole attack, wormhole attack, sinkhole attack, grey hole attack, selective forwarding attack, hello flood attack, misdirection attack, internet smurf attack, spoofing attack.
4	Transport layer	De-synchronization, transport layer flooding attack.
5	Application layer	Spoofing, alter routing attack, false data ejection, path-based DoS.

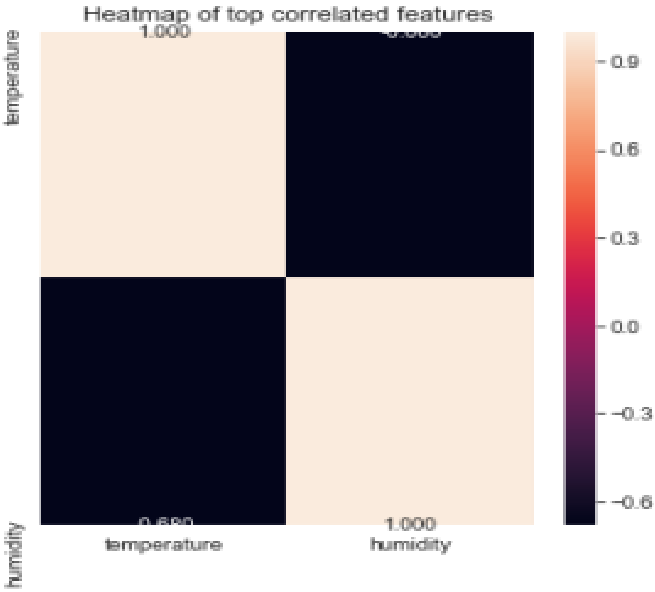
Inside the gateway, the data of the sensor node will be saved in influxdB and visualized as a graph and transmitted continuously to the cloud where it is visualized as shown in the Graph 2. This figure illustrates environmental information gathering data as a greenhouse area from 12 January to 16 June 2020.

Graph 1: Agropolis results from the 12 to 16 of January 2020



Graph 2: Agropolis results from the 12 to 16 of January 2020

The correlation between variables after processing on Python is shown in Graph 3. The low correlation between temperature and humidity can be confirmed.



Graph 3: Correlation matrix

During the time period, data from sensor nodes are successfully sent to the gateway with a data loss of 17 percent. Users could get a better understanding of the greenhouse area environment according to the graphs.

V. CONCLUSION

The general aim of this thesis has been development a Wireless Sensor Network, continuous monitoring using IoT. The study is using wireless network sensor technology to implement a monitoring system in the agricultural sector. Gateway and sensor nodes contribute to the proposed system. it is designed for supporting farmer. Although WSNs are object of extensive scientific and technological advances and can effectively achieve distributed data collection for IoT applications, their wide scale use is still limited by perceived low reliability, limited autonomy, high cost and reduced accessibility to application domain experts. It is a technological revolution based on dynamic innovation in several essential areas such as wireless sensors and nanotechnology, representing the future of the IoT, computing, and communication. Areas of application include a wide variety of industries such as management, electricity, industrial control, retail, utility healthcare. In a new expression defined as the future of the Internet, the IoT directs a new future surrounded by small smart objects that interact with the environment, communicate with each other, and are controlled over the Internet. We consider WSN platform an essential enabler for effective application design: fast development with low effort and cost, reliable designs based on extensive reuse, flow accessible to application domain experts, and offering maintainable extensive technology coverage.

REFERENCES

1. Bhisham Sharma (2020), "Integration of WSN with IoT Applications: A Vision, Architecture, and Future Challenges", Integration of WSN and IoT for Smart Citie,ISSNno:2319-5045,Pages.79-102.DOI:10.1007/978-3-030-38516-3_5
2. Rustam Pirmagomedov (2018), "IoT Based Earthquake Prediction Technology: 18th International Conference, NEW2AN 2018, and 11th Conference, ruSMART 2018, St. Petersburg, Russia, August 27–29, 2018, Proceedings",Internet of Things, Smart Spaces, and Next Generation Networks and Systems,ISSNno:0302-9743,Pages.535-546.DOI:10.1007/978-3 -030-01168-0_48
3. Hamid Errachdi (2023), "Bridging the Gap: Challenges and Opportunities of IoT and Wireless Sensor Networks in Marine Environmental Monitoring", Eng. Proc.,ISSNno:2673-4591,Vol.58(1),Pages.102.https://doi.org/10.3390/ecsa-10-16158
4. Shancang Li (2014), "Internet of Things in Industries: A Survey",IEEE Transactions on Industrial Informatics,ISSNno:1941-0050,Vol.10(4),Pages.22 33-2243.DOI:10.1109/TII.2014.2300753
5. Rashmi M. Jogdand (2020), "A Survey on Internet of Things (IoT), Industrial IoT (IIoT) and Industry 4.0",International Journal of Computer Applications, ISSNno:0975-8887,Vol.175(27),Pages.20-27.DOI:10.5120/ijca2020920790
6. Mohammad S. Obaidat (2020), "A Comparative analysis of IoT based products, technology and integration of IoT with cloud computing",IET Networks,ISSNno:2047-4962,Vol.9(2),DOI:10.1049/iet-net.2019.0180

7. Jun-Hong Cui (2006), "The challenges of building mobile underwater wireless networks for aquatic applications",IEEE Network,ISSNno:1558-156X,Vol.20 (3),DOI:10.1109/MNET.2006.1637927
8. Guang Yang (2019), "Challenges and Security Issues in Underwater Wireless Sensor Networks",Procedia Computer Science,ISSNno:1877-0509,Vol.147, Pages.210-216.https://doi.org/10.1016/j.procs.2019.01.225
9. Seokjoo Shin (2022), "Survey on Multi-Path Routing Protocols of Underwater Wireless Sensor Networks: Advancement and Applications",Electronics,ISSN no:1450-5843,Vol.11(21),Pages.3467.https://doi.org/10.3390/electronics1121 3467
10. Mamoona Majid (2022), "Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review",Sensors (Basel),ISSNno:1424-8220,Vol.22(6),Pages.2087. doi:10.3390/s22062087

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |