IoT and WSN bridge: Application and Challenges

Abstract: **-With the increasing demand of Wireless Sensor Network (WSN) innovations, it cuts numerous zones mobile communication, cloud computing and embedded system in modern living. IoT(Internet of Things) is widely used in environmental condition monitoring, Logistic Support and interfacing sensors and actuators wirelessly, which can control from far distance. This offers the capacity to control the world from a corner of a room. wherein sensors and actuators operate reliably with the help of IoT(Internet of Things). For data transmission and controlling a system RF was used vastly but some technical burden, IoT replace the era of RF. For example, RF implanted sensor and actuator hubs, the IoT has offered out of its earliest stages and is the following progressive innovation in changing the Internet into a completely incorporated Future Internet. This paper exhibits a technical overview of WSN(Wireless sensor Networking) with Cloud driven vision for overall execution of IoT (Internet of Things) along with the drawbacks and challenges.**

Keywords- IoT (Internet of Things); of WSN (Wireless sensor Networking); RF; sensors and actuators.

I. TOOLS OF IOT TECHNOLOGIES

A) Wireless Sensor Network (WSN)

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. The propagation technique between the hops of the network can be routing or flooding. In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year, for example IPSN, SenSys, and EWSN. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

B) Middleware

Middleware refers to a software layer interfered between computer applications to make it simpler for the software developers to achieve the real time communication between input and output. Its main features are that, it was used as hiding the details of different technologies is fundamental to free IoT developers from software services that are not directly to the specific IoT application. Middleware expanded its popularity in the year of 1980s because of its vital role in shortening the addition of different legacy technologies into new ones. It also added the development of new services with the DCS (distributed computing system).

C) Cloud Computing:

Both IoT (Internet of things) and th**e** Cloud computing have a gratis relationship. The IoT (Internet of things) provides enormous amounts of data whereas cloud computing is required to

offering a pathway to store the and prevent the data loss. Thus, cloud computing helps to increase the efficiency and control movement of IoT (Internet of things)**.** Cloud computing also increase the agility and the speed while making the resources very easy for the developers. One can save the valuable time and the cost during operating data and can use the data without any redundancy by using Cloud Computing.

II. NETWORK APPLICATIONS

IoT and WSNs were originally motivated by military applications, which range from large - scale acoustic surveillance systems for ocean surveillance to small networks of unattended ground sensors for ground target detection.

A) Environment Monitoring

In environmental monitoring, sensors are used to monitor a variety of environmental parameters or conditions. Environmental monitoring is one of the earliest applications of sensor networks. Sensors can be deployed on the ground or under water to monitor air or water quality. For example, water quality monitoring can be used in the hydrochemistry field. Sensors can be used to monitor biological or chemical hazards in locations, for example, a chemical plant or a battlefield. Sensors can be densely deployed in an intended region to detect natural or non - natural disasters. For example, sensors can be scattered in forests or revivers to detect forest fi res or floods Air or Water Quality Monitoring.

B) Military Application

Due to ease of deployment, self - configurability, untended operation, and fault tolerance, sensor networks will play more important roles in future military C3I systems and make future wars more intelligent with less human involvement. Sensors can be mounted on unmanned robotic vehicles, tanks, fighter planes, submarines, missiles, or torpedoes to guide them around obstacles to their targets and lead them to coordinate with one another to accomplish more effective attacks or defenses. Sensor nodes can be deployed around sensitive objects, for example, atomic plants, strategic bridges, oil and gas pipelines, communication centers, and military headquarters, for protection purpose. Sensors can be deployed for remote sensing of nuclear, biological, and chemical weapons, detection of potential terrorist attacks, and reconnaissance. Sensors can be deployed in a battlefield to monitor the presence of forces and vehicles, and track their movements, enabling close surveillance of opposing forces.

C) Health Care Application

WSNs can be used to monitor and track elders and patients for health care purposes, which can significantly relieve the severe shortage of health care personnel and reduce the health care expenditures in the current health care systems. Wearable sensors can be integrated into a wireless body area network (WBAN) to monitor vital signs, environmental parameters, and geographical locations, and thus allow long - term, noninvasive, and ambulatory monitoring of patients or elderly people with instantaneous alerts to health care personal in case of emergency, immediate reports to users about their current health statuses, and real - time updates of users ’ medical records.

D) Industrial Process Control

Tiny sensors can be embedded into the regions of a machine that are inaccessible by humans to monitor the condition of the machine and alert for any failure. For example, wireless sensors can be instrumented to production and assembly lines to monitor and control production processes. Chemical plants or oil refiners can use sensors to monitor the condition of their miles of pipelines. In industry, WSNs can be used to monitor manufacturing processes or the condition of manufacturing equipment

E) Security and Surveillance

For example, acoustic, video, and other kinds of sensors can be deployed in buildings, airports, subways, and other critical infrastructure, for example, nuclear power plants or communication centers to identify and track intruders, and provide timely alarms and protection from potential attacks.

F) Home Intelligence

WSNs can be used to provide more convenient and intelligent living environments for human beings. Wireless sensors can be embedded into a home and connected to form an autonomous home network. Wireless sensors can be used to remotely read utility meters in a home, for example, water, gas, or electricity, and then send the readings to a remote center through wireless communication. In addition to the above applications, self - configurable WSNs can be used in many other areas, for example, disaster relief, traffic control, warehouse management, and civil engineering.

III. NETWORK DESIGN OBJECTIVES

A) A) Small Node Size

Reducing node size is one of the primary design objectives of sensor networks. Sensor nodes are usually deployed in a harsh or hostile environment in large numbers. Reducing node size can facilitate node deployment, and also reduce the cost and power consumption of sensor nodes.

B) Low Node Cost

Reducing node cost is another primary design objective of sensor network. Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers and cannot be reused, it is important to reduce the cost of sensor nodes so that the cost of the whole network is reduced.

C) Low Power Consumption

Reducing power consumption is the most important objective in the design of a sensor network. Since sensor nodes are powered by battery and it is often very difficult or even impossible to change or recharge their batteries, it is crucial to reduce the power consumption of sensor nodes so that the lifetime of the sensor nodes, as well as the whole network is prolonged.

D) Self – Configurability

In sensor networks, sensor nodes are usually deployed in a region of interest without careful planning and engineering. Once deployed, sensor nodes should be able to autonomously organize themselves into a communication network and reconfigure their connectivity in the event of topology changes and node failures.

E) Scalability

In sensor networks, the number of sensor nodes may be on the order of tens, hundreds, or thousands. Thus, network protocols designed for sensor networks should be scalable to different network sizes.

F) Adaptability

In sensor networks, a node may fail, join, or move, which would result in changes in node density and network topology. Thus, network protocols designed for sensor networks should be adaptive to such density and topology changes.

G) Reliability

For many sensor network applications, it is required that data be reliably delivered over noisy, error - prone, and time - varying wireless channels. To meet this requirement, network protocols designed for sensor networks must provide error control and correction mechanisms to ensure reliable data delivery.

H) Fault Tolerance

Sensor nodes are prone to failures due to harsh deployment environments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of self - testing, self - calibrating, self-repairing, and self - recovering.

I) Security

In many military applications, sensor nodes are deployed in a hostile environment and thus are vulnerable to adversaries. In such situations, a sensor network should introduce effective security mechanisms to prevent the data information in the network or a sensor node from unauthorized access or malicious attacks.

J) Channel Utilization

Sensor networks have limited bandwidth resources. Thus, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization.

K) QoS Support

In sensor networks, different applications may have different quality - of - service (QoS) requirements in terms of delivery latency and packet loss. For example, some applications, for example, fi re monitoring, are delay sensitive and thus require timely data delivery. Some applications, for example, data collection for scientific exploration, are delay tolerant but cannot stand packet loss. Thus, network protocol design should consider the QoS requirements of specific applications.

IV. NETWORK DESGIN CHALLENGES

A) Limited Hardware Resources

Sensor nodes have limited processing and storage capacities, and thus can only perform limited computational functionalities. These hardware constraints present many challenges in software development and network protocol design for sensor networks, which must consider not only the energy constraint in sensor nodes, but also the processing and storage capacities of sensor nodes.

B) Massive and Random Deployment

Most sensor networks consist of a large number of sensor nodes, from hundreds to thousands or even more. Node deployment is usually application dependent, which can be either manual or random. In most applications, sensor nodes can be scattered randomly in an intended area or dropped massively over an inaccessible or hostile region. The sensor nodes must autonomously organize themselves into a communication network before they start to perform a sensing task.

C) Dynamic and Unreliable Environment

A sensor network usually operates in a dynamic and unreliable environment. On one hand, the topology of a sensor network may change frequently due to node failures, damages, additions, or energy depletion. On the other hand, sensor nodes are linked by a wireless medium, which is noisy, error prone, and time varying. The connectivity of the network may be frequently disrupted because of channel fading or signal attenuation.

D) Diverse Application

Sensor networks have a wide range of diverse applications. The requirements for different applications may vary significantly. No network protocol can meet the requirements of all applications. The design of sensor networks is application specific.

E) Limited Energy Capacity

Sensor nodes are battery powered and thus have very limited energy capacity. This constraint presents many new challenges in the development of hardware and software, and the design of network architectures and protocols for sensor networks. To prolong the operational lifetime of a sensor network, energy efficiency should be considered in every aspect of sensor network design, not only hardware and software, but also network architectures and protocols.

V. CONCLUSION

VI. REFERENCES