SRI MUTHUKUMARAN INSTITUTE OF TECHNOLOGY
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
ODD SEMESTER JULY'23-DEC'23
(Regulation – 2021)
V SEM/ III YEAR
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
CEC368 - IOT BASED SYSTEMS DESIGN
QUESTION BANK

UNIT II -MIDDLEWARE AND PROTOCOLS OF IOT

PART A

1.What is wireless sensor networks?
WSNmiddlewareisakindofmiddlewareprovidingthedesiredservices for sensor-based pervasive computing applications thatmake use of a WSN and the related embedded operating systemorfirmwareofthesensornodes.

2.List out the four major components of WSN.
1.Programmingabstractionsdefinetheinterfaceofthemiddlewareto the application programmer.
2.System services provide implementations to achieve the abstractions.
3.Runtime support servesasanextensionoftheembeddedoperatingsystemtosupportthe middleware services.
4.QoS mechanisms define the QoS constraints of the system.

3.Write the challenges faced in middleware WSN.
Manychallengesariseindesigningmiddlewareforwsnduetothefollowingreasonsandmore:

- Limitedpowerandresources,e.g.,batteryissues
- Mobileanddynamicnetworktopology
- Heterogeneity,variouskindsofhardwareandnetworkprotocols
- Dynamicnetworkorganization,ad-hoccapability

4.Write the examples of WSN.

MagnetOS
IMPALA
Cougar
SINA
MIRES
MQTT-S
MiLAN

5.**Write the examples of WSNMiddlewareandWSNLanguages.**

Agilla	eCos	MagnetOS	SINA
AutoSec	EMW	MANTIS	SOS
Bertha	Enviro-Track	Mate	TinyDB
BTnutNut/OS	EYESOS	MiLAN	TinyGALS
WSNLanguages			
c@t	DCL (DistributedCompositionalLanguage)	galsC	nesC

Protothreads	SNACK	SQTL	

6.List the fundamental resources of agilla.

Agilla provides two fundamental resources on each node: an neighbor list and a tuple space.The neighor list contains the addresses o fneighboring nodes. This is necessary for agents to decide where they want to move or clone to next.

7. What is BACnet protocol.

BACnet stands for Data Communication Protocol for **B**uilding **A**utomation and **C**ontrol **Net**works. Unlike most other protocols that began as private implementations followed by standardization efforts, BACnet was built from the ground up as an independent, royalty-free, open standard control and automation protocol. The standard committee was chaired by university professors until 2004, its goal was to harmonize data types and formats, data exchange primitives, and common application services. Several open source.

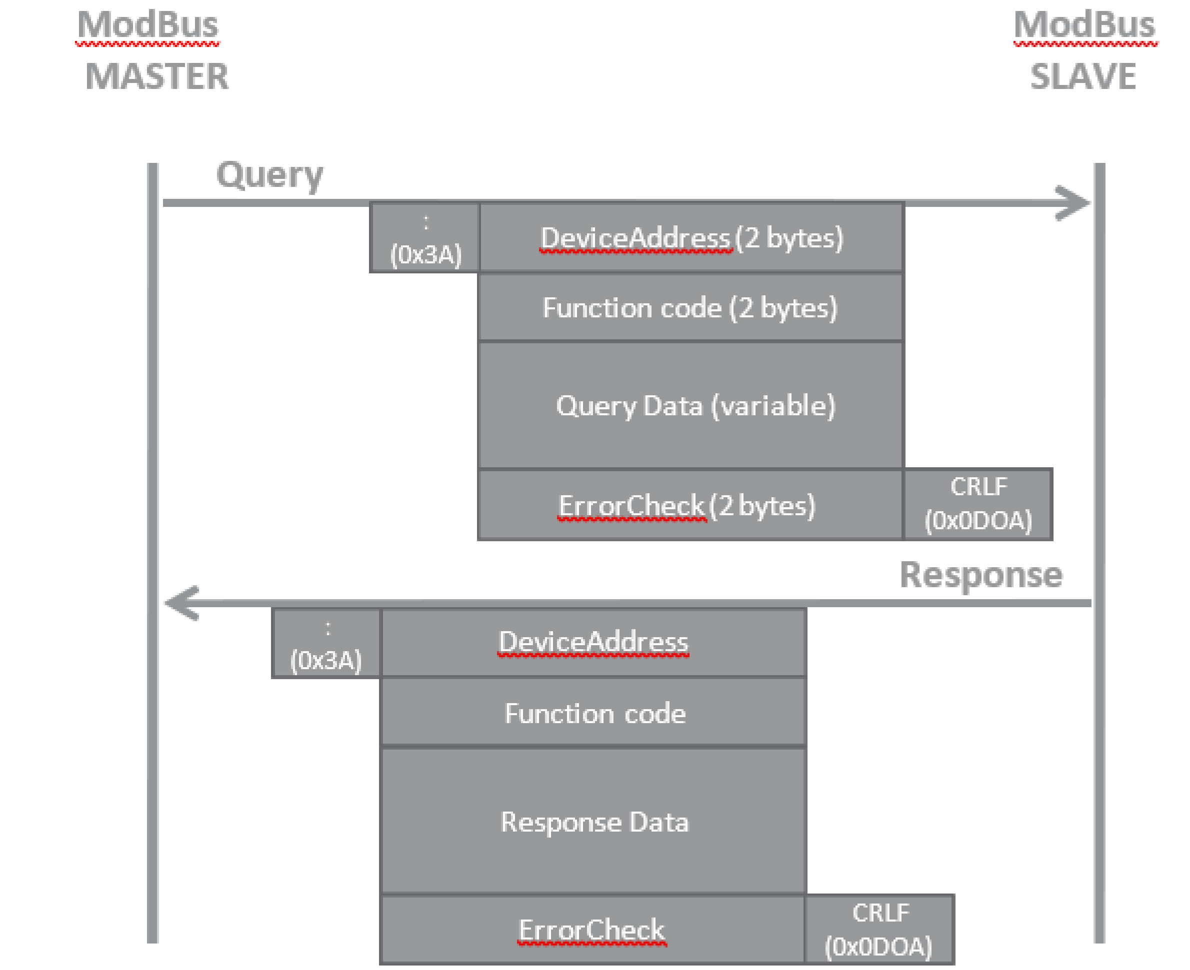
8. **Mention the ModBus Standardization used in iot protocols.**

- ModBus is a trademark of Modicon inc (Schneider Electric group), which also maintains the standard.
- ModBus is an application layer messaging protocol that provides client/server communicationbetween devices connected on different types of buses or networks. Becauseof its simplicity, ModBus has become one of the *de-facto* standards for industrial serial message-based communications since 1979.
- ModBus typically runs on top of RS 232, RS 442 point to point or RS 485 point to multipoint links. The ModBus/TCP specification, published in 1999 defines an IP-based link layer for ModBus frames.
- ModBus devices communicate using a master-slave model: one device, the master, can initiate transactions (called *queries*), which can address individual slaves or be broadcast to all slaves. The slaves take action as specified by the query, or return the requested data to the master.

9. List out the Modbus address used in iot.

ModBus Addresses: ModBus messages begin by the target 8-bit address that can takeany decimal value between 1 and 247. 0 is used for broadcasts. The address field of themessage frame contains two characters in ASCII mode, or 8 bits in RTU Mode. Eachquery contains the address of a specific slave. When it responds, the slave includes itsownaddress inthemessage.

10. Draw the ModBusmessageframing(ASCIImode).



11.Define konnex protocol.

The Konnex (or KNX) Association was set up in 1999 on the merger between three formerEuropeanassociationspromotingintelligenthomesandbuildings:

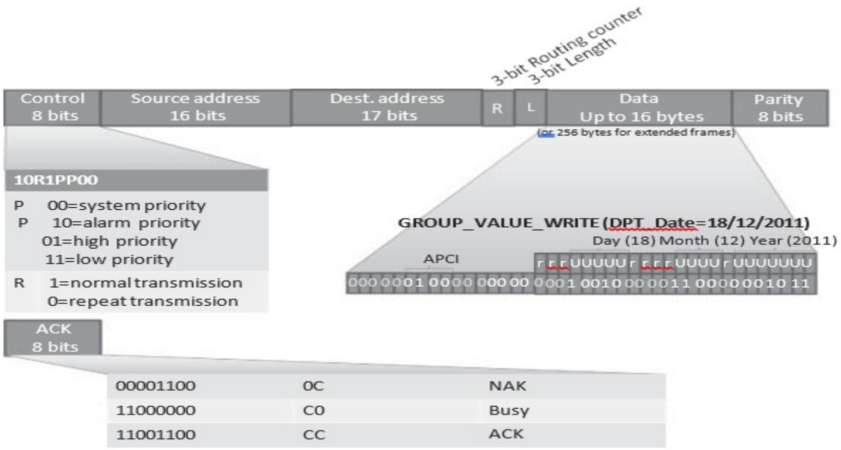
·BatibusClubInternational(BCIFrance)promotingthe Batibussystem;
·TheEuropeanInstallationBus Association(EIBA)promotingtheEIB system;
·European HomeSystems Association (Holland) promotingtheEHS system.

The goal of the KNX Association was to define and offer certification services for the KNXopen standard, while offering legacy support and certification cervices for Batibus, EIB[1]andEHS.

12.Mention the konnex protocol standardization

In order to standardize the specifications, the KNX association cooperates with CENELECTC205.TheKNXprotocolhasbecomeaninternationalstandardinEuropeasEN50090(media and management procedures), EN 13 321-1 (media) and EN 13 321-2 (CEN,KNXnet/IP).

13.Draw the KNXtelegramformat.



14.Define GroupObjects

The process information of KNX functional blocks (input, output or parameter) may bepublishedasagroupobject(GO).Agroupobjectmaybereadorwrittenoverthebusviadedicated multicast service primitives. The KNX specification of each functional blockdefineswhichoftheinputs,outputsandparametersmay,ormust,bepublishedasagroupobject .

15.Draw the KNX interface objects and properties.

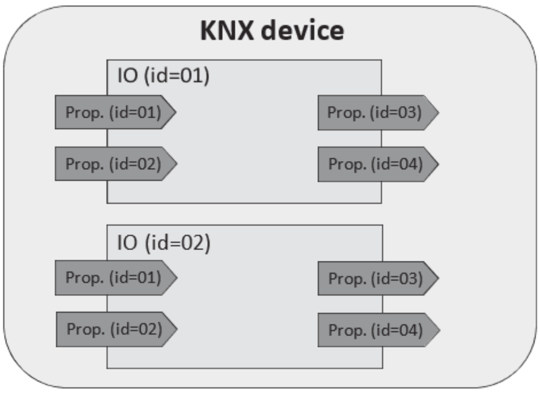


Figure 6.6 KNX interface objects and properties.

16.**What is ZigBee Device Object.**

The **ZigBee Device Object (ZDO)** layer is a specific application running on endpoint 0,designedtomanagethestateoftheZigBeenode.TheZDOapplicationimplementstheinterfaces defined by the ZigBee device profile (ZDP, application profile ID 0x0000).These primitives encapsulate the 802.15.4 network formation primitives of the Zig-Bee network layer (node discovery, network joining), as well as additional primitivessupportingtheconceptofbinding.

17.ZigBeeClusterLibrary(ZCL)wasalateadditiontoZigBee,specifiedina

separatedocument.Itconsistsinalibraryofinterfacespecifications(clustercommandsandattributes) thatcanbeusedinpublicandprivateapplicationprofiles.

18.ZigBeeCoordinator. Thisnodetypecorrespondstoa802.15.4fullfunction device (FFD) having a capability to form a network and become a 802.15.4 PANcoordinator.ZigBeecoordinatorscanformanetwork,orjoinanexistingnetwork(in which case they become simple ZigBee routers). In nonbeacon-enabled 802.15.4networks, coordinators are permanently listening devices that act as routers, and sendbeaconsonlywhenrequestedbyabroadcastbeaconrequestcommand.

19.Mention the BACNET protocol application.

BACnet protocol is used in all types of automated building systems. So, there are interoperable products available within different categories like security, fire, lighting, elevators, HVAC, etc. This protocol simply addresses the interoperability goal through simply defining a general working model of automation devices, a technique used for defining the data that they include, & also a technique used for explaining protocols that a single device can utilize to inquire one more device to execute some preferred action

20.Define BACnet/IP

This is normally used with existing VLAN & WAN networks. So the devices can connect directly to hubs or Ethernet switches. This LAN is a high-performance & fast type, but very costly. BACnet/IP utilizes UDP/IP for compatibility through existing IP infrastructure. Once BACnet/IP is utilized with several IP subnets, then extra device functionality known as BBMDs (BACnet Broadcast Management Devices) is necessary to handle broadcast messages of inter-subnet BACnet.

21.Diffrentiate BACnet and ModBus.

BACnet Protocol	**Modbus**
It was developed by ASHRAE.	It was developed by Modicon Inc.
Bacnet is used for communication across devices.	Modbus is used for communication between devices.
Its transmission modes are; IP, Ethernet, Zigbee & MS/TP.	Its transmission modes are; ASCII, RTU, and TCP/IP.

22.List out the advantages of bacnet protocol.

The **advantages of the Bacnet Protocol** include the following.

- BACnet protocol is particularly designed for building automation as well as control networks.
- It doesn’t depend on present LAN or WAN technologies.
- It is an American National Standard & a European pre-standard.
- It is scalable completely from small single building applications to universal networks of devices.
- The implementers of BACnet can securely include non-standard extensions as well as enhancements without influencing existing interoperability.

23.Mention the disadvantage of Bacnet protocol.

The **disadvantages of the Bacnet Protocol** include the following.

The main drawback of the BACnet protocol was a compliant problem. So because of this issue, the BTL (BACnet Testing Laboratories) was introduced in the year 2000. BTL is compliance & and independent testing organization. The main intention of this is to test the products of BACnet to verify compliance with the standard. Once approved; the product will get the logo of BTL.

24. List out the advantage and disadvantage of modbus protocol.

The advantages of Modbus are; **simple installation, simple to use, reliable communication, open specifications**, etc. The disadvantages of Ethernet are mobility, installation, connections, expandability, etc. The disadvantages of Modbus are; It doesn't have any object form however space is reserved only for addresses.

PART B

1.Explain in detail about the architecture of SCADA Middleware

TheconceptofMAN(M2Mareanetwork)wasintroducedin3GPP/ ETSI'sMTCspecification.Thisconceptalsoappliesto other pillar segments of IoT. However, not all IoT applicationswilluseacellularnetwork.Infact,mostofthetraditionalSCADAapplicationshavebeenusinglocalwirelinenetworksforcommunications.Theremoteterminalunits(RTUs),pro-grammablelogiccontrollers(PLCs),orevenprocesscontrolsystems(PCSs)communicatetothe SCADAmiddlewareserverviagateways(similartoMANbutallwired)thataggregatedatafromdifferentwiredfieldbuses.TheSCADAsystemisaccessedinaLANenvironment(sometimesxDSL,cable,WiFi,orWiMaxcanbeused)beforeitisintegratedintothecorpo-ratebackofficesystem.

Consideringthatmanyofthefieldbusesalsosupport IP,such as Modbus TCP/IP, BacNet IP, and others, it is possibleoreasierthanwirelessnetworkstoadoptanall-IPapproachtoimplementSCADAapplications.Thisapproachhasbeenusedinsomeoftheprojectsdonebytheauthorinbuildingmanagementsystems.Figure5.3(redrawnbasedonconceptsfrom [264]) depicts the role of SCADA middleware in such ascenarioinmoredetail.

CompaniesprovidingsuchSCADAmiddlewareproductsincludethefollowing:

- Central Data Control: CDC provides the software platformIntegra,whichutilizesdataagentstotranslateprotocolsfromdifferentbuildingsystemcomponentsintosinglemanagementsystem.
- Elutions: Its Control Maestro product has a SCADA heri-tage.SCADAmaybebestknownforindustrialprocessesbutisalsodeployedforinfrastructure(watertreatmentplants,gaspipelines,etc.)aswellasfacilitysystems.ControlMaestrois web-based,useshuman–machine

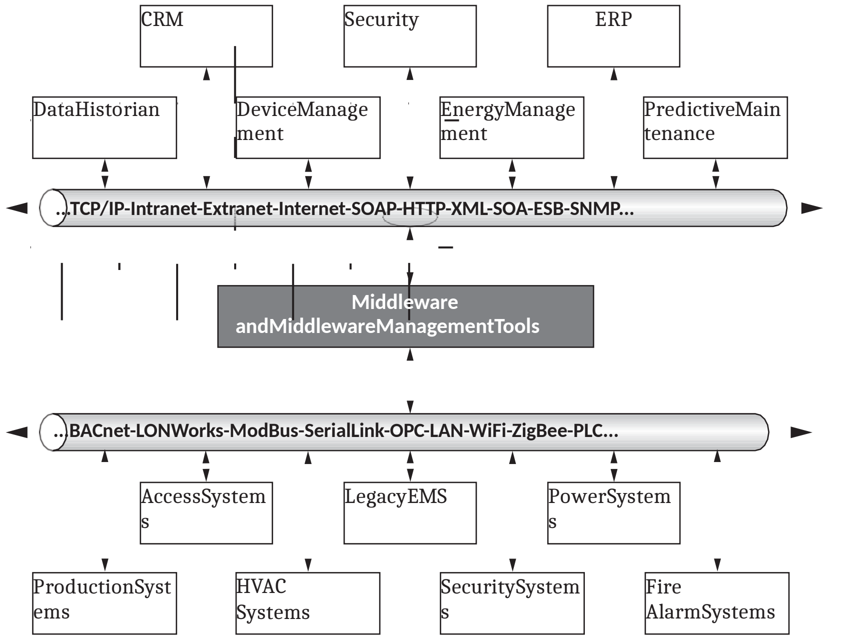


Figure5.3 SCADAmiddlewarearchitecture.

interfaces(HMI),andisabletodeliverreal-timeandhistoricalinformation.

- RichardsZeta:RZ’smiddlewaresolutionisacombination ofsystemcontrollersandsoftware.
- Tridium:ItprovidestheNiagaraJava-basedmiddlewareframework and JACE hardware controllers. The Niagaraplatformprovidesprotocoltranslationforarangeofsystemsandthetools to build applications. NiagarahasopenAPIstoallNiagaraservicesandanextensiblecomponentmodel(XML)thatenabledevelopmentof applicationsbythirdparties.Italsoprovidessupportforweb-servicesdatahandlingandcommunicationswithenterpriseapplications.

Withthedevelopmentofwirelesstechnologies,systemshavebeendevelopdthatblendwirelesswithwiredcommu-nicationinSCADAapplications.SensiLink^{TM}isamiddleware andsoftwaresuitefromMeshNeticsthatlinkswirelesssensornetworks with SCADA systems. Sensor data collected from thenodes is channeled through RS232, RS485, USB, Ethernet, orGPRSgatewaytotheSensiLinkserver.

OPCmiddlewareproductsareoneoftheimportantcom-municationslayerSCADAmiddlewarethataredesignedtoenhanceanyOPCstandards-basedapplications.Originally,OPCwas defined as a standardizedsolutionfortherecur-ring task of connecting PC-based SCADA/HMI applicationswithautomationandprocesscontroldevices.Today,theOPCstandardhasevolvedintoarobustdatacarrierabletotrans-portentireenterpriseresourceplanningdocumentsandevenvideosignals.

OPCisforWindowsonly(detailsaboutthestandardisdiscussed in Chapter 6). Tridium is arguably the first SCADAmiddlewarebasedonJavatechnology.RecentdevelopmentshaveintegratednewtechnologiessuchasJavaandiOS(appli-cationstore)tobuildOSplatformagnosticmiddlewareforbroaderIoTapplications;adoptingnewtechnologiesforSCADAisatrend.

2.EXPLAIN IN DETAIL ABOUT THE RFID Middleware ARCHITECTURE

RFIDnetworkingsharesasimilarthree-tieredcommunica-
tionarchitecture(asshowninFigure5.4).RFIDreadersarethegatewayssimilartoMAN.Datafro
mthereadersgotothecorporateLANandthenaretransmittedtotheInternetas
needed.However,justlikethescenariosofM2MandSCADA,mostcurrentRFIDsystemsstopatt
hecorporateLANlevelandareIoTsystemsonly.

RFIDmiddleware(includingtheedgemiddlewareoredge-
ware)iscurrentlynodoubtthemostwell-defined,comprehen-
sive,standardizedmiddlewarecomparedwiththeotherthreepillarsegmentsofIoT.Before2004,a
nRFIDmiddleware-basedsystemwasdefinedbyEPCglobal,whichincluded:

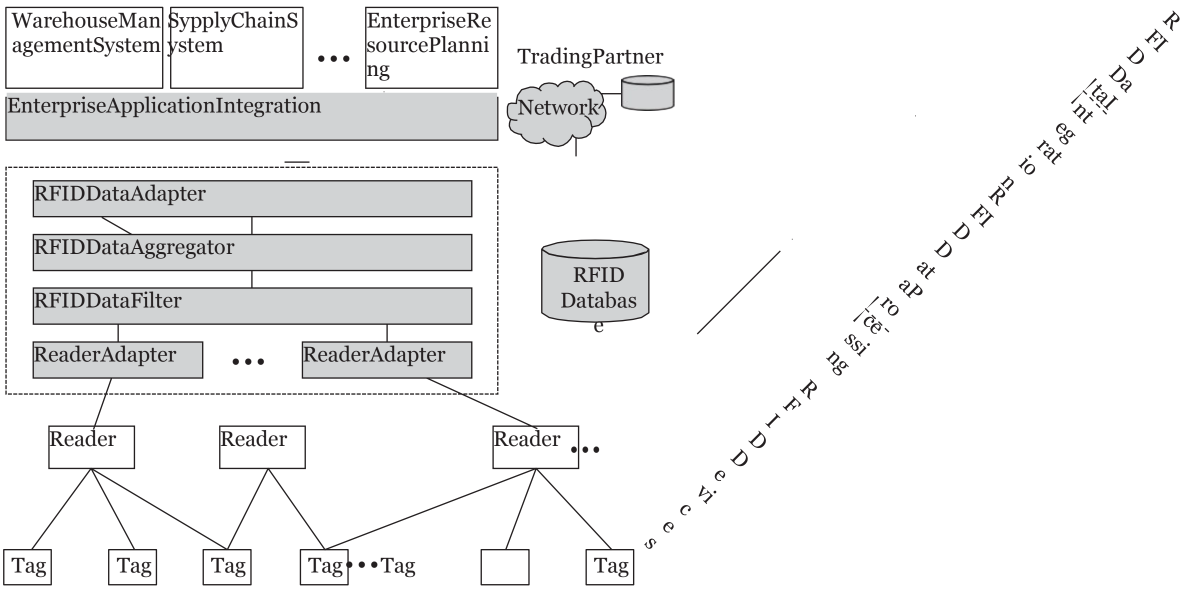


Figure 5.4 RFIDarchitecture.(FromQuanZ.Sheng,KerryL.Taylor,Zakaria Maamar, and Paul Brebner, "RFID Data Management: Issues,Solutions,andDirections,"inLuYan,YanZhang,LaurenceT.Yang,andHuanshengNing(Eds.),*TheInternetofThings:FromRFIDtotheNext-GenerationPervasiveNetworkedSystems*,NewYork:AuerbachPublications,2008.)

- Aformatforthedatacalledphysicalmarkuplanguage(PML),basedonXML(Figure5.5isanexample)
- AninterfacetotheserverscontainingPMLrecords
- AdirectoryservicecalledONS(objectnamingservice),analogoustotheDNS.Givenatag'sEPC,theONSwill providepointerstothePMLserverscontainingrecordsrelatedtothattag.

However, since 2004, the unified PML schema has beendropped [51] due to, most likely, practical reasons becausemostRFIDsystemsarestillinthe"IntranetofThings"scope.Using the generic PML/ONS approach would involve over-head and sacrifice efficiency. Instead, the PML-like schema wasleftttotheverticalapplicationstodefinetheirownXML

```
<pmlcore:Sensor>
  <pmluid:ID>urn:epc:1:4.16.36</pmluid:ID>
  <pmlcore:Observation>
    <pmlcore:DateTime>2002-11-06T13:04:34-06:00</pmlcore:DateTime>
    <pmlcore:Tag>
      <pmluid:ID>urn:epc:1:2.24.400</pmluid:ID>
      <pmlcore:Sensor>
        <pmluid:ID>urn:epc:1:12.8.128</pmluid:ID>
        <pmlcore:Observation>
          <pmlcore:DateTime>2002-11-06T11:00:00-
06:00</pmlcore:DateTime>
          <pmlcore:Data>
            <pmlcore:XML>
              <TemperatureReading xmlns="http://sensor.example.org/">
                <Unit>Celsius</Unit>
                <Value>5.3</Value>
              </TemperatureReading>
            </pmlcore:XML>
          </pmlcore:Data>
        </pmlcore:Observation>
        <pmlcore:Observation>
          <pmlcore:DateTime>2002-11-06T12:00:00-
06:00</pmlcore:DateTime>
          .........
        ..........
```

Figure5.5 Physicalmarkuplanguagesample.

scheme.Consequently,theoverallsystemarchitectureofRFIDhas evolved from a dedicated structure to a more generic,openarchitecture.

However,thePMLapproachisbelievedtobeagoodIoTdatarepresentationmethodthatshoul d be used when thedayofthefull-blownIoTsystemcomes.OthereffortssuchasM2MXML(fromBiTX)andoBIX(anOASISstand ard)areunderwaythataretryingtobuildagenericIoTdataschema,whichisdiscussedinthenextc hapter.

An example of commercial RFID middleware product isIBM's WebSphere Sensor Events. WebSphere Sens

or Events deliv-ers new and enhanced capabilities to create a robust, flexible,andscalableplatformforcapturingnewbusinessvaluefromsen-sordata.WebSphereSensorEventsistheplatformforintegratingnew sensor data, identifying the relevant business events fromthat data using situational event processing, and then integratingandactinguponthoseeventswithSOAbusinessprocesses.

TheblendingorconvergenceofdifferentpillarIoTapplica-tionstobuildcross-segmentIoTsystemsisatrendthathasbeendemonstrated[228],inwhichunifieddatarepresentati onandassociatedcommunicationmiddlewarebecamemoreandmoreimportant.

3.EXPLAIN IN DETAIL ABOUT THE WSN Middleware architecture

Middlewarealsocanrefertosoftwareandtoolsthatcanhelphidethecomplexityandheterogeneity oftheunderlyinghard-wareandnetworkplatforms,easethemanagementofsystemresources, and increase the stableness of application executions.WSNmiddlewareisakindofmiddlewareprovidingthedesiredservices for sensor-based pervasive computing applications thatmake use of a WSN and the related embedded operating systemorfirmwareofthesensornodes[57].Inmostcases,WSNmiddle-wareisimplementedasembeddedmiddlewareonthenode[82].

Itshouldbenotedthatwhilemostexistingdistributedsystemmiddlewaretechniquesaimatpro vidingtransparencyabstractionsbyhidingthecontextinformation,WSN-basedapplicationsareusuallyrequiredtobecontextaware,asmen-tionedinChapter1[18].

A complete WSN middleware solution should include

fourmajorcomponents:programmingabstractions,systemservices,runtimesupport,andquality ofservice(QoS)mechanisms.
Programmingabstractionsdefinetheinterfaceofthemiddlewareto the application programmer. System services provide imple-mentations to achieve the abstractions. Runtime support servesasanextensionoftheembeddedoperatingsystemtosupportthe middleware services. QoS mechanisms define the QoS con-straints of the system. The system architecture of WSN middle-wareisshowninFigure5.6.

Middleware for WSN should also facilitate development,maintenance,deployment,andexecutionofsensing-basedapplications.ManychallengesariseindesigningmiddlewareforWSNduetothefollowing reasonsandmore:

- Limitedpowerandresources,e.g.,batteryissues
- Mobileanddynamicnetworktopology
- Heterogeneity,variouskindsofhardwareandnetworkprotocols
- Dynamicnetworkorganization,ad-hoccapability

WSNmiddlewareisdesignedusinganumberofapproachessuchasvirtualmachine,mobileag ents,databasebased,message-oriented,andmore.Examplemiddlewareareasfollows[83]:

- MagnetOS (Cornell University): power-aware, adaptive;thewholenetworkappearsasasingleJVM,standardJavaprogramsarerewrittenby MAGNETasnetworkcompo-nents,andcomponentsmaythenbe“injected”intothenetworkusingapower-optimizedscheme.
- IMPALA:modular;efficiencyofupdatesandsupportdynamicapplications;applicationa daptionwithdifferentprofilespossible;energyefficient;usedintheZebraNetprojectforwi ldlifemonitoring.
- Cougar:representsallsensorsandsensordatainarelationaldatabase; control of sensors and extracting data occursthroughspecialSQL-likequeries;decentralizedimplementa-tion;messagepassingbasedoncontrolledflooding.
- SINA (system information networking architecture): basedonaspreadsheetdatabasewhereinthenetworkisacollectionofdatasheetsandcellsarea ttributes;attribute-based naming;queriesperformedinanSQL-likelanguage;decentralizedimplementationbasedonclustering.
- MIRES: publish/subscribe; multihop routing; additionalservice (e.g., data aggregation); sense—advertise over P/Sandroutetosink.
- MQTT-S(MessageQueueTelemetryTransportforSensors,IBM): a publish/subscribe messagingprotocol for WSN,withtheaimofextendingtheMQTTprotocolbeyond the reach of TCP/IP infrastructures (non-TCP/IP networks,suchasZigbee)forsensorandactuatorsolutions;acom-mercialproduct.
- MiLAN: provides a mechanism that allows for the adapta-tion of different routing protocols; sits on top of multiplephysicalnetworks;actsasalayerthatallowsnetwork-specificplug-instoconvertMiLANcommandstoprotocol-specificonesthatarepassedthroughtheusualnetworkprotocolstack;cancontinuouslyad apttothespecificfeaturesofwhichevernetworkisbeingusedinthecommunication.

TheWSNmiddlewareisconsideredtobe“proactive”middlewareinthemiddlewarefamily.A morecomprehensivelistofexistingWSNmiddlewareplatforms,software/ OS,andprogramminglanguagesisshowninTable5.3.AcomparisonofsomeoftheWSNmiddle wareisavailable[84].

Asanexample,theAgillamiddlewareisexaminedhereinmoredetail(Figure5.7).TheAgilla[22 9]runsontopofTinyOSandallowsmultipleagentstoexecuteoneachnode.Thenum-berofagentsisvariableandisdeterminedprimarilybythe

Table5.3 SampleWSNMiddlewareandWSNLanguages

WSNMiddleware			
Agilla	eCos	MagnetOS	SINA
AutoSec	EMW	MANTIS	SOS
Bertha	Enviro-Track	Mate	TinyDB
BTnutNut/OS	EYESOS	MiLAN	TinyGALS
COMiS	FACTS	Mire	TinyOS
Contiki	Global SensorNetworks (GSN)	Netwiser	t-Kernel
CORMOS	Impala	OCTAVEX	VIPBridge
COUGAR	jWebDust	SenOS	
DSWare	LiteOS	SensorWare	
WSNLanguages			
c@t	DCL (DistributedCo mpositionalLa nguage)	galsC	nesC
Protothreads	SNACK	SQTL	

amountofmemoryavailable.Eachagentisautonomousbutsharesmiddlewareresourceswithoth eragentsinthesystem.

Agillaprovidestwofundamentalresourcesoneachnode:aneighborlistandatuplespace.Then eighborlistcontainstheaddressesofneighboringnodes.Thisisnecessary foragentstodecidewheretheywanttomoveorcloneto next.The tuple space provides an elegant decoupled-styleofcommunicationbetweenagents.Itisasharedmemoryarchitecturethatisaddressedbyfiel d-matchingratherthanmemoryaddresses.Atupleisasequence of typed dataobjectsthatisinsertedinto the tuple space. The tupleremainsinthetuplespaceeveniftheagentthatinserteditdiesormovesaway.Later,anothera gentmayretrievethetuplebyissuingaqueryforatuplewiththesamesequence

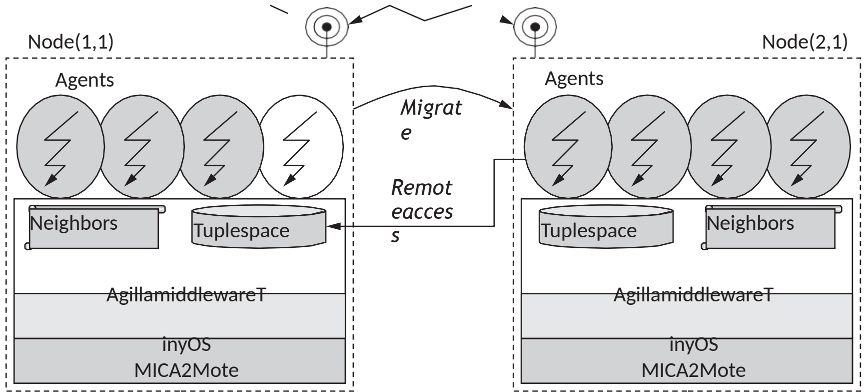


Figure5.7 TheAgillamiddlewaremodel.(FromChien-LiangFok,Gruia-Catalin Roman, and Chenyang Lu, “Software Support forApplication Development in Wireless Sensor Networks,” in PaoloBellavista and Antonio Corradi (Eds.), *The Handbook of MobileMiddleware*,NewYork:AuerbachPublications,2006.)

offields.Notethattuplespacesdecouplethesendingagentfromthereceivingagent:theydonothav etobeco-located,orevenawareofeachother’sexistence,forthemtocom-municate.Thisisbasicallyafault-tolerantdistributedcom-putingtechnology.

AlloftheaboveWSNmiddlewareareatthedeviceleveluptothegateways(equivalenttotheMA NofMTC).Mostofthemareresearchprojectsconductedatuniversitiesandresearchinstitutionsw ithafewexperimentalusesandoflimitedcom-mercialvalue.Thissituationisverymuchliketheresearchonparallelcomputingarchitectureoneo rtwodecadesago.

4. Explain in detail about the BACNET protocol with neat diagram.

BACnet stands for Data Communication Protocol for **B**uilding **A**utomation and **C**ontrol **Net**works. Unlike most other protocols that began as private implementations followed by standardization efforts, BACnet was built from the ground up as an independent, royalty-free, open standard control and automation protocol. The standard committee was chaired by university professors until 2004, its goal was to harmonize data types and formats, data exchange primitives, and common application services. Several open source.

Standardization

The BACnet standardization effort began in 1987 during a Standard Project Committee meeting of ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers). BACnet became an ISO standard in 2003 (ISO 16 484-5). In January 2006 the BACnet Manufacturers Association and the BACnet Interest Group of North America combined their operation in a new organization called BACnet International , which provides conformance testing services (BACnet Testing Laboratories) and promotes the adoption and development of the standard.

United States

BACnet became a standard in 1995 as ASHRAE/ANSI standard 135 and a conformance testing method was standardized in 2003 as BSR/ASHRAE Standard 135.1. The last revision of the standard was published in 2010.

Europe

BACnet was adopted in 2003 by CEN (Comit´e Europ´een de Normalization, http://www.cen.eu) Technical Committee 247, for the management level and automation level. For the Automation level, it coexists with EIBnet (Konnex), at the Field level, CEN adopted Konnex (merger of three European protocols EIB (European Installation bus), Batibus, EHS), and LonWorks/LONTalk.

Europe has a specific European user and interest group: http://www.big-eu.org.

Interworking

BACnet ability to interwork with other technologies has always been a key concern, and BACnet does provide enough flexibility to allow mapping of other common protocols to a BACnet model. However, there are often many ways of providing such a mapping, and there is a need to formally specify a standard mapping in order to ensure interoperability of interprotocol gateway implementations:

– BACnet interoperability with Konnex (KNX) control protocol has been specified in Annex H/5.

– BACnet interoperability with ZigBee has been specified in Annex X.

Technology

BACnet focuses on the network layer and above. At the presentation layer, it uses ASN.1 syntax1 for the definition of all data structures and messages (application protocol data units or APDUs). The BACnet transport layer adds routing information to these APDUs, and the resulting messages may be carried on top of virtually any link layer, using the adaptation functions provided by the BACnet network layer.

Physical Layer
BACnet upper layers are independent from the underlying physical layer, facilitating the implementation of BACnet on most popular networks. BACnet physical layers have been defined for ARCNET, Ethernet, IP tunneling (defined for routers interconnecting BACnet segments over IP in Annex H), BACnet/IP (devices are IP aware and can communicate directly over IP networks), RS-232 (BACnet Point to Point), RS-485 (withBACnet specific Master-Slave/Token Passing LAN technology, up to 32 nodes on 1200 m, at 76 kbit/s on shielded twisted pairs), and LonWorks/LonTalk.

Link Layer
BACnet can be implemented directly on top of the LonTalk or IEEE802.2 (Ethernet and ArcNet) data link layers. It also defines a data link layer (Point to Point PTP) for RS232 serial connections, and a MS/TP data link layer for RS-485.
For IP or other network technologies that can be used as link layers, the standard defines a BACnet virtual link layer (BVLL) that formalizes all the services that a BACnet device might require from the link layer, such as broadcasts.
For instance, BACnet devices may implement the IP BVLL, which encapsulates the required control information not readily available from the native IP link layer (e.g., a flag indicating whether the message was received as a unicast or broadcast), in a BACnet virtual link control information (BVLCI) header . Thanks to the IP BVLL, BACnet devices become full-fledged BACnet IP devices, able to communicate directly over IP without a need for an "Annex H" router. Similarly, a BACnet device could implement an ATM, frame relay or ISDN BVLL in order to become a native node in these networks.
On many link layers, broadcasts are difficult or have their own limitations. BACnet has a concept of a "BACnet broadcast management device" (BBMD), which implements the broadcast requirements of BACnet for the selected link layer, for example, it may convert a BACnet broadcast into IP-based multiunicast and/or broadcast messages. Devices can register with the BBMD to receive broadcast messages dynamically.

Network Layer
BACnet is primarily defined as a network layer protocol, which defines the network addresses required for the routing of messages.

BACnet Services
Each service uses a set of messages supporting the related communication needs. The messages are defined using ASN.1 syntax (ANSI/ASHRAE 135 clause 21) and exchanged using standard remote operation primitives (request, indication, response, confirm):
_ ***Alarm and event services:*** BACnet provides multiple event reporting options: objects may support "intrinsic reporting" (e.g., report an event periodically, report error conditions, status updates), or may be configured by means of *Event enrollment* object to report specific conditions such as a change of value (*COV reporting*), or a value out of range. The latter mechanism, called *algorithmic reporting* implements a subscribe-notify model for events. The objects that requested to be notified are listed in *Notification Class* objects
The following service primitives are defined for event management and reporting:
AcknowledgeAlarm
(self-explanatory), **ConfirmedCOVNotification** (*Change of value* event notification primitive in which receivers must report the success or failure of actions taken as a result of the event), **UnconfirmedCOVNotification**, **ConfirmedEvent-Notification**, **UnconfirmedEventNotification**, **GetAlarmSummary** (BACnet events can be flagged as alarms, in which case a list of active alarms is returned by this primitive), **GetEnrollmentSummary** (returns a list of event-notifying objects according to specified filters, such as objects with an active event enrollment from another object), **GetEventInformation** (returns a list of active event states within a device),

LifeSafetyOperation (e.g., silence a siren), **subscribeCOV** (subscribe to *Change of value* notifications for an object), **SubscribeCOVProperty** (subscribe to *Change of value* notifications for a property).
_ ***File access services:*** read and write primitives are atomic, that is, a single operation is executed at a time.

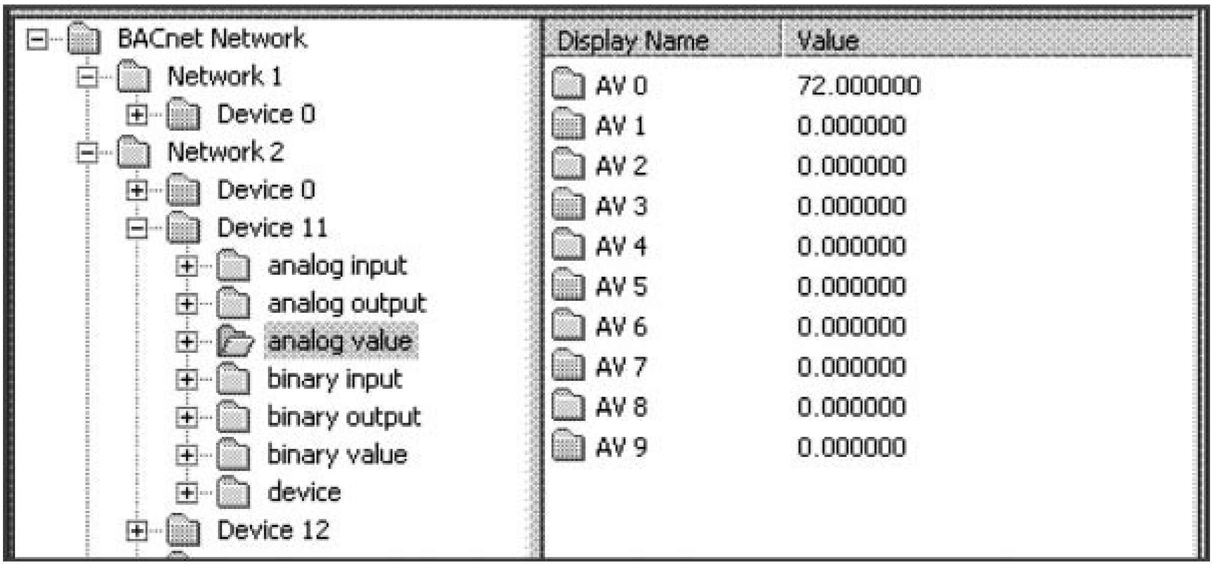
BACnet Security

BACnet device A supporting security can request a session key from a key server for a future communication with device B. The key server will generate a session key SKab and transmit it securely to A and B (encrypted with the private keys of A, respectively B). BACnet uses 56-bit DES encryption.

Device A may then authenticate a future transaction with B: A and B authenticate each other by exchanging challenges (based on random numbers encrypted with the session key), the challenge message includes the identifier (InvokeID) of the future transaction to be authenticated.

A may also ensure the confidentiality of the future transaction by encrypting the corresponding application message with the session key.

BACNET SERVICES



5.**Explain in detail about MODBUS protocol**

ModBus Standardization

ModBus is a trademark of Modicon inc (Schneider Electric group), which also maintains the standard.

ModBus is an application layer messaging protocol that provides client/server communication between devices connected on different types of buses or networks. Because of its simplicity, ModBus has become one of the *de-facto* standards for industrial serial message-based communications since 1979.

ModBus typically runs on top of RS 232, RS 442 point to point or RS 485 point to multipoint links. The ModBus/TCP specification, published in 1999 defines an IP-based link layer for ModBus frames.

ModBus devices communicate using a master-slave model: one device, the master, can initiate transactions (called *queries*), which can address individual slaves or be broadcast to all slaves. The slaves take action as specified by the query, or return the requested data to the master.

ModBus Message Framing and Transmission Modes

The transmission mode defines the framing and bit encoding of the messages to be transmitted on the ModBus network. In a given ModBus network, all nodes must use the same mode and serial parameters:
_ In the ***ASCII Transmission Mode***, each byte is encoded on the serial link as 2 ASCII characters. Each ASCII character is sent separately as 1 start bit, 7 data bits, zero or one parity bit, one or two stop bits. The message is framed by a starting ":" ASCII byte, and

ends with a “CR-LF” byte sequence (see Figure 5.1).
_ In the ***RTU*** **(remote terminal unit)** *transmission mode*, the message is transmitted in a continuous stream. Each 8-bit byte is framed by 1 start bit, 8 data bits, zero or one parity bit, one or two stop bits. The message itself starts after a silent period of at least 3.5 character times.

ModBus/TCP

The ModBus/TCP specification can be found at http://www.eecs.umich.edu/∼modbus/ documents/Open_ModbusTCP_Standard.doc
ModBus/TCP provides TCP/IP access to the ModBus functionality. Each ModBus Request/response is sent over a TCP connection established between the master and the slave, using well-known port 502. The TCP connection may be reused for several query/ response exchanges.
The byte content of the ModBus request and response frames (i.e. without framing startstop-parity bits specific to the serial physical layer) is simply transported over the TCP connection, in big indian order.

6.**Explain in detail about KNX protocol**

KNX Technology Overview

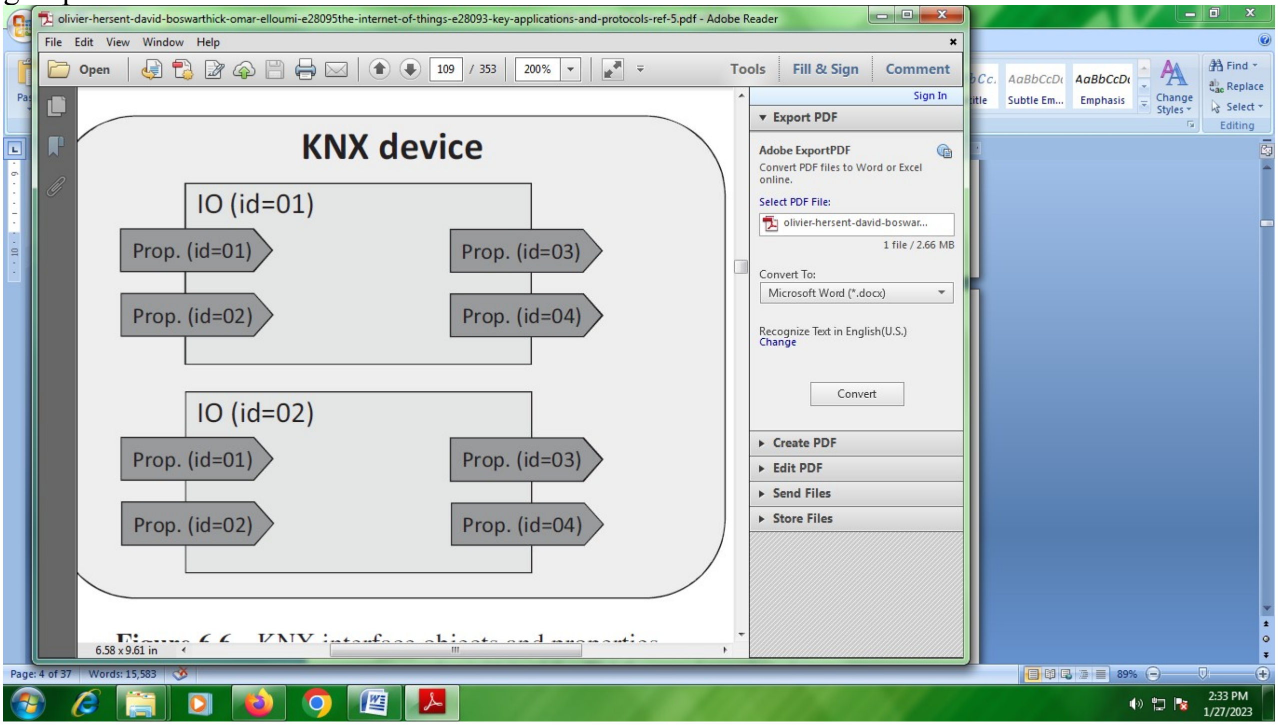
The overall KNX architecture is documented in Vol 3, part 3/1. The KNX architecture is decentralized: nodes can interact with other nodes without the need for a central controller.

The protocol stack uses the OSI model with a null session and presentation layer. It is based on the original work of EIB, which is therefore backward compatible to KNX. KNX standardizes the protocol, but also the data model (EN 50 090-3-3, KNX volume 3/7) for basic types (integer and float values, percentage) and common device functions such as switching, dimming, blinds control, HVAC and so on .

Physical Layer

The physical layer of KNX is specified in Vol 3, Chapter 3/3/1 of the specifications. KNX can use a variety of physical layers
– **TP1**3**: Twisted pair** (Chapter 3/2/2). TP was the first physical layer that was defined as part of EIB, and is still the dominant physical layer used in KNX deployments.
The TP bus provides both power and communication, using inductive coupling (Figure 6.2). A twisted-pair installation is made of lines, each line is composed of up to 4 line segments interconnected by repeaters, and each segment interconnects up to 64 devices. Lines are interconnected by line couplers (LC). The line couplers interconnect to the KNX backbone via a backbone controller (BbC), and the devices that can be accessed via a given BbC are part of the same KNX area (or zone). Line couplers and backbone controllers act as routers, that is, filter the messages that they relay based onthe destination address and the domain id (when present). The address space allows up to 15 areas (Figure 6.1), each with 15 lines, and a KNX TP installation can manage a maximum of 61 249 devices.
The transmission begins with a start bit (0), followed by a application octet, a parity bit, a stop bit (1) and a mandatory pause (11). The theoretical throughput is 9600 bps.
– **PL110 Over PLC**4 (Chapter 3/2/3). PL110 uses a FSK modulation scheme and was also part of the original EIB specification. Each PLC line can have up to 64 devices. Since PLC is inherently a broadcast open media, the separation of domains (the portion of the KNX network logical topology over which the data signals of one physical layer type propagate) is ensured by a 48-bit domain address, in addition of the zone/line/node Id address (see TP1 for a description of these addresses).
– **Over RF** (Chapter 3/2/5 defined in 2001). This physical layer uses the 868-870 MHz band (Figure 6.3).
The KNX-rf 1.1 specification was updated in 2010, introducing a “push button” and easy controller mode setup specification, and using a 1% duty cycle on the center frequency 868.3 MHz: this version is called “KNX-rf ready”. It allows bidirectional communication with low duty cycle devices by sending a 4.8-ms preamble for

transmissions. Devices are preconfigured with group addresses for multicast communication, and unicast communication uses an "extended group address" composed of the group address of the sender and its serial number.



7. Explain in detail about zigbee architecture.

Zig Bee Architecture

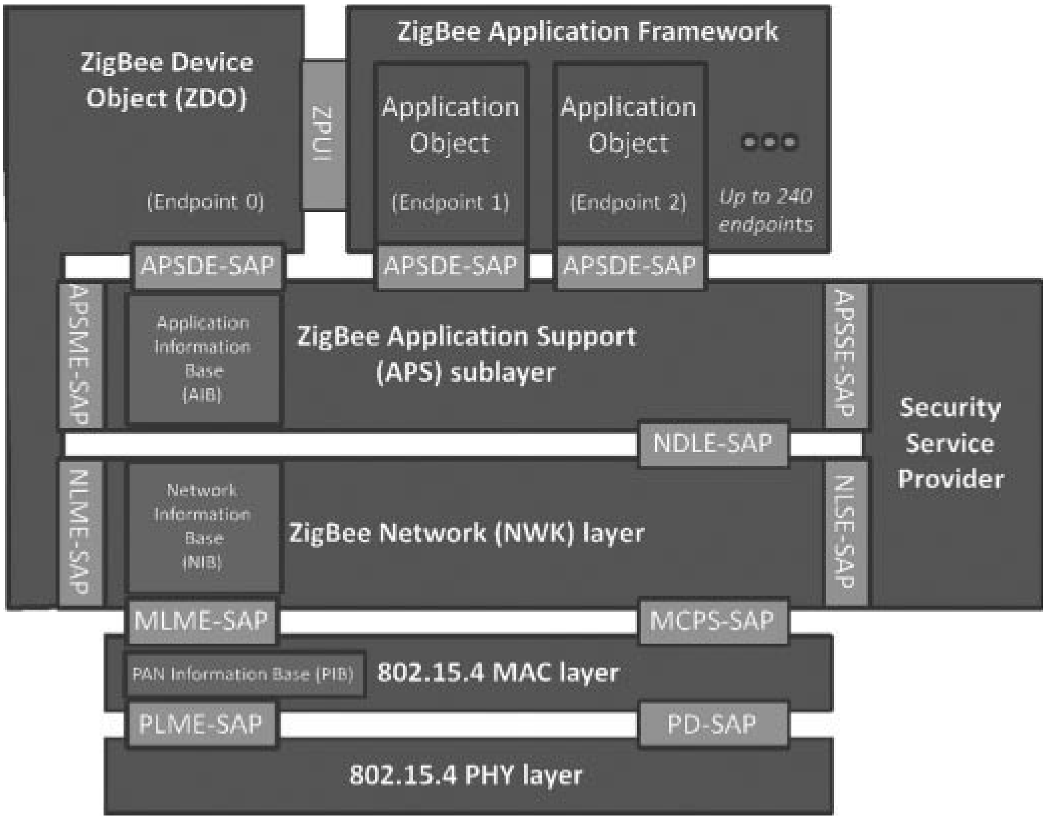
ZigBee sits on top of 802.15.4 physical (PHY) and medium-access control (MAC) layers, which provide the functionality of the OSI physical and link layers.

So far ZigBee uses only the 2003 version of 802.15.4. All existing ZigBee commercial devices use the 2.4 GHz S-Band as the 2003 version of 802.15.4 does not allow sufficient bandwidth on other frequencies. The 2006 version adds improved data-transfer rates for 868 MHz and 900 MHz but is not yet part of the ZigBee specification.

802.15.4 offers 16 channels on the 2.4 GHz, numbered 11 to 26. ZigBee uses only the nonbeacon-enabled mode of 802.15.4, therefore all nodes use CSMA/CA to access the network, and there is no option to reserve bandwidth or to access the network deterministically.

ZigBee restricts PAN IDs to the 0x0000 – 0x3FFF range, a subset of the 802.15.4 PAN ID range (0x0000-0xFFFE).

All unicast ZigBee commands request a hop by hop acknowledge (optional in 802.15.4), except for broadcast messages.



Management of end to end acknowledgements. The application layer supports acknowledgements independently of the link layer acknowledgements of 802.14.4.
The APS manages retries and duplicate filtering as required, simplifying application programming.
• Fragmentation.
Also, as part of the application support sublayer management entity, or APSME:
• Group addressing: the APSME allows to configure the group membership tables of each endpoint ID, and forwards messages addressed to a group ID to the application objects with relevant endpoint IDs.
• Security: management of keys.
– The **ZigBee Device Object (ZDO)** layer is a specific application running on endpoint 0, designed to manage the state of the ZigBee node. The ZDO application implements the interfaces defined by the ZigBee device profile (ZDP, application profile ID 0x0000). These primitives encapsulate the 802.15.4 network formation primitives of the ZigBee network layer (node discovery, network joining), as well as additional primitives supporting the concept of binding (see Section 7.5.2.2).
– The **ZigBee Cluster Library (ZCL)** was a late addition to ZigBee, specified in a separate document. It consists in a library of interface specifications (cluster commands and attributes) that can be used in public and private application profiles.

8.Explain in detail about zigbee node types

ZigBee Node Types

The ZigBee node types listed below are not mutually exclusive. A given device could implement some application locally (e.g., a ZigBee power plug) acting as a ZigBee End Device, and also be a ZigBee router and even a ZigBee coordinator.
– **ZigBee End-Device (ZED):** this node type corresponds to the 802.15.4 reduced function device. It is a node with a low duty cycle (i.e. usually in a sleep state and not permanently listening), designed for battery operation. ZEDs must join a network through a router node, which is their parent.
– **ZigBee router (ZR):** this node type corresponds to the 802.15.4 full function device (FFD). ZigBee routers are permanently listening devices that act as packet routers, once they have joined an existing ZigBee network.
– **ZigBee Coordinator (ZC):** this node type corresponds to a 802.15.4 full function

device (FFD) having a capability to form a network and become a 802.15.4 PAN coordinator. ZigBee coordinators can form a network, or join an existing network (in which case they become simple ZigBee routers). In nonbeacon-enabled 802.15.4 networks, coordinators are permanently listening devices that act as routers, and send beacons only when requested by a broadcast beacon request command.

prominentresearchersonparallelarchitectureatthattime.HehasbeendoingresearchonWSNsincethewaneofparallelarchitectureresearch.Infact,someoftheWSNarchitectureandmiddlewareideasareinheritedfromparallelcomputerarchitectures,whichwillmostlikelydiminishthesamewayastimepassesby,especiallytheadhocwirelessnetworks(theymayhavegreatervalueinmilitaryuses).

Nevertheless,oncethedatafromtheadhocmeshWSNreachesthegateways,orifthewirelesssensorsaredirectlyconnectedtothehigher-tiernetworks,theremainingprocessandroutetoreachtheInternetofThingswillbethesameastheotherpillarsegmentsofIoT.TheWSNmiddlewareatthesystemlevelmaybethesameasSCADAorM2MorRFIDsys-tems,whichsharethesamethree-tieredarchitecturediscussedinthelastthreesections.