

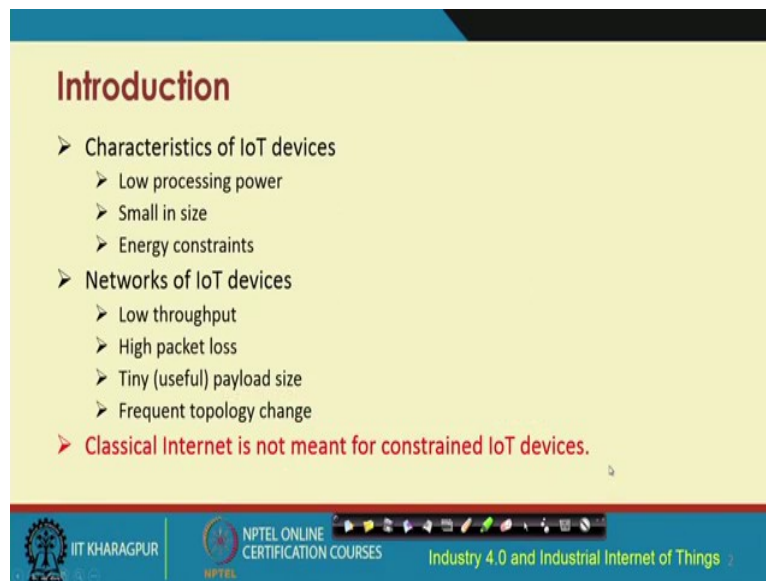
Introduction to Industry 4.0 and Industrial Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 04
Introduction: IoT Networking - Part I

In this lecture, we are going to discuss the networking issues in IoT. In the previous lectures, we looked at the connectivity issues, what are the challenges, what are the solutions, that are available.

From a networking point of view, we will look at the different other aspects of setting up IoT systems, what are the solutions again that are there, in order to address.

(Refer Slide Time: 01:23)



The slide is titled "Introduction" and lists the following points:

- Characteristics of IoT devices
 - Low processing power
 - Small in size
 - Energy constraints
- Networks of IoT devices
 - Low throughput
 - High packet loss
 - Tiny (useful) payload size
 - Frequent topology change

➤ **Classical Internet is not meant for constrained IoT devices.**

The slide footer includes the IIT Kharagpur logo, NPTEL Online Certification Courses logo, and the text "Industry 4.0 and Industrial Internet of Things".

The typical network, that is encountered, consists of a source, a data source or multiple data sources consisting of sensors, typically sensors, RFIDs, which collect data and interact with the physical environment, and then the data is sent elsewhere for further processing. Based on the processing the data is analyzed.

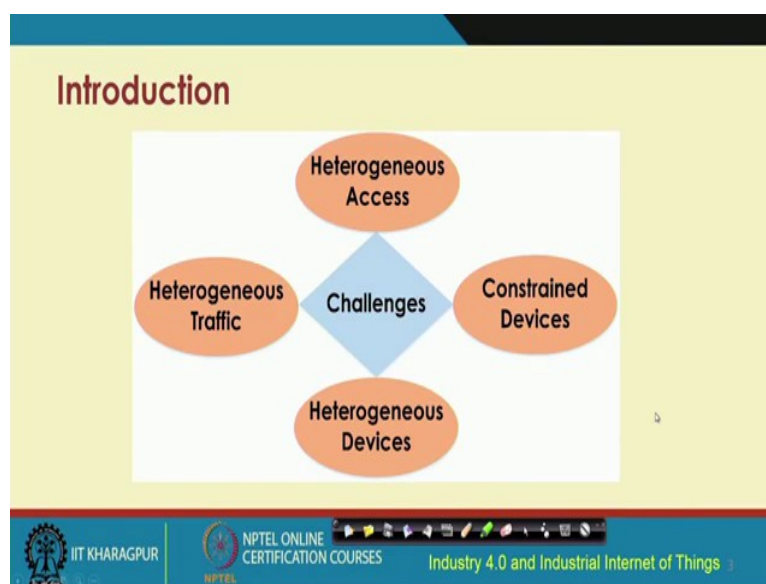
Some system would be actuated; it may or may not be actuated or there may not be any actuation associated with the system at all. We have seen both of these types in the previous lectures.

From a network point of view, how to set up the network let us try to understand. These IoT devices will have very low processing power. They are very small in size, energy constraints, typically, battery operated. Because of the small size, the batteries that are used are also small. And due to the electrochemical limitation of the batteries; these batteries will have a very limited lifetime. So, you need to have solutions at the hardware, software, and algorithmic level, which will consume very low power.

From a network point of view, specifically, we need systems, protocols, solutions, algorithms, which will consume extremely low energy. IoT devices are energy constraint; they are small in size, and have very limited processing power. So, network protocols that are designed for use in IoT should be designed accordingly keeping these constraints in mind.

These networks typically support very low throughput; they have high packet loss. These networks typically operate in environments which are very much noisy, there are a lot of interferences, consequently the packet loss is also high. And they have small, useful payload size and in most cases, these networks also exhibit the behavior of frequent changes in their topology. Therefore, it is a highly constraint dynamic kind of scenario and coming up with networking solutions is a huge challenge in these in these systems. So, classical internet that is based on TCP/IP; the classical internet that we all use is not meant for these constraint IoT devices.

(Refer Slide Time: 05:25)



From a holistic viewpoint, the challenges can be classified into different types. We have challenges with respect to access; there is heterogeneous access, heterogeneous traffic flowing through these networks. There is heterogeneity in the devices, vendors, specifications, standards, protocols, that are used by these devices working in the networks. In all respects these are constraints.

(Refer Slide Time: 06:23)

Introduction

- Analogy
 - Roots - Communication Protocol and device technologies
 - Trunk- Architectural Reference Model (ARM)
 - Leaves – IoT Applications
- Goal
 - To select a minimal set of **roots** and propose a potential **trunk** that enables the creation of a maximal set of the **leaves**.

Source: FhG, I. M. L., et al. "Internet of things-architecture iot-a deliverable d1. 3-updated reference model for iot"

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Introduction to Intern

To think about IoT; let us think about let us you know think about a tree. So, this analogy has been taken from the source that is given on the slide. The tree has the roots, trunk, and leaves. The different IoT applications like smart health care, smart transportation, smart cities, smart energy, smart retail, smart home, smart cities overall. All these smart things that we talk about in the context of IoT are analogous to the leaves of a tree.

At the very bottom of the tree are these roots; these roots are like communication protocols and device technologies. So, these protocols and device technologies are sort of like the roots of the tree; technologies such as Bluetooth, ZigBee, Z-Wave, Wi-Fi, sensors, and actuators are the different roots of the tree.

Considering the IoT applications, on the very top and the roots like the technologies, protocols that I just mentioned; the objective is to come up with a suitable trunk that will support these applications and we will connect with the roots of the tree. The trunk is basically the architectural reference model of IoT, the arm model of IoT. So, overall from an optimization kind of viewpoint; the goal can be stated that we need to select a minimum set

of roots and propose a potential trunk that enables the creation of maximum set of leaves. This can be thought of like the overall objective; the optimization objective.

(Refer Slide Time: 08:35)

Enabling Classical Internet for IoT Devices

- Proprietary non-IP based solution
 - Vendor specific gateways
 - Vendor specific APIs
- Internet Engineering Task Force (IETF) IP based solution
 - Three work groups
 - IPv6 over Low power Wireless Personal Area Networks (6LoWPAN)
 - Routing Over Low power and Lossy networks (ROLL)
 - Constrained RESTful Environments (CoRE)

Source: I. Ishaq, et al., "IETF standardization in the field of the internet of things (IoT): a survey", *J. of Sens. and Act. Netw.*, vol. 2 (2013): 235-287.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

IoT offers non-IP based proprietary, remains like vendor specific solutions or we can think of using the IP based solutions, based on the IETF protocols. On the contrary, IETF IP based solutions; where there are different initiatives to support IoT like; the 6LoWPAN; which talks about IPv6 over LoWPAN, which is low power wireless personal area network.

So, IPv6 over 6LoWPAN is one such technology; one such protocol, which is being worked upon by a specific 6LoWPAN working group. Likewise, there are other working groups talking about the adaptation of IoT requirements to the internet.

ROLL is basically routing over low power lossy networks. CoRE is constraint restful environments. 3 different working groups are there, like this there are multiple different initiatives in order to have support of IoT over IP; that means, the existing internet.

(Refer Slide Time: 10:59)

Proprietary non-IP based solution

- Drawbacks
 - Limited flexibility to end users: vendor specific APIs
 - Interoperability: vendor specific sensors and gateways
 - Limited last-mile connectivity

Source: I. Ishaq, et al., "IETF standardization in the field of the internet of things (IoT): a survey", J. of Sens. and Act. Netw. 2, vol. 2 (2013): 235-287.

IIT KHARAGPUR NPTEL ONLINE CERTIFICATION COURSES Industry 4.0 and Industrial Internet of Things

Different sensor systems could be using proprietary solutions, proprietary protocol stack. On the other side, different devices such as laptops, desktops, then these PDAs and many others, which typically in the existing framework use the existing TCP/IP protocol stack of the internet.

We need to come up with a solution which can fit these proprietary solutions to the existing framework of the internet; which is supporting laptops, PDAs and different other wireless devices. This is holistic framework that we are talking about, but the drawback of this non-IP based solutions is limited flexibility to end users. These are vendor specific API's, so there is limited flexibility to the end users.

In terms of interoperability there are vendor-specific sensors; vendor-specific gateways. You know it is like some sensor nodes, some IoT devices pick one vendor specific language. Let us say, that somebody speaks English, somebody speaks French, somebody speaks Hindi; how they can talk to each other? There is no common language, there is no interoperability between them.

So, in order to conquer this kind of heterogeneity; you need to have a common framework which will make these disparate devices follow different proprietary standards talk to each other. Interoperability is this issue which talks about conquering this challenge of heterogeneity in all different respects.

Because these are not models which are supposed to scale up; so that the scalability can be maintained. There it is a IP scalable solution; unlike this proprietary vendor specific solutions, which are non-scalable.

(Refer Slide Time: 13:52)

IETF IP based solution

- Three work groups
 - IPv6 over Low power Wireless Personal Area Networks (6LoWPAN)
 - By header compression and encapsulation it allows IPv6 packets to transmit and receive over IEEE 802.15.4 based networks.
 - Routing Over Low power and Lossy networks (ROLL)
 - New routing protocol optimized for saving storage and energy.
 - **Constrained RESTful Environments (CoRE)**
 - Extend the Integration of the IoT devices from network to service level.

The slide includes a footer with logos for IIT KHARAGPUR, NPTEL ONLINE CERTIFICATION COURSES, and Industry 4.0 and Industrial Inte. A small video inset shows a speaker in the bottom right corner.

So, we have different IP-based solutions as well typically follow different initiatives by IETF, 6LoWPAN, ROLL and CoRE are 3 different important ones.

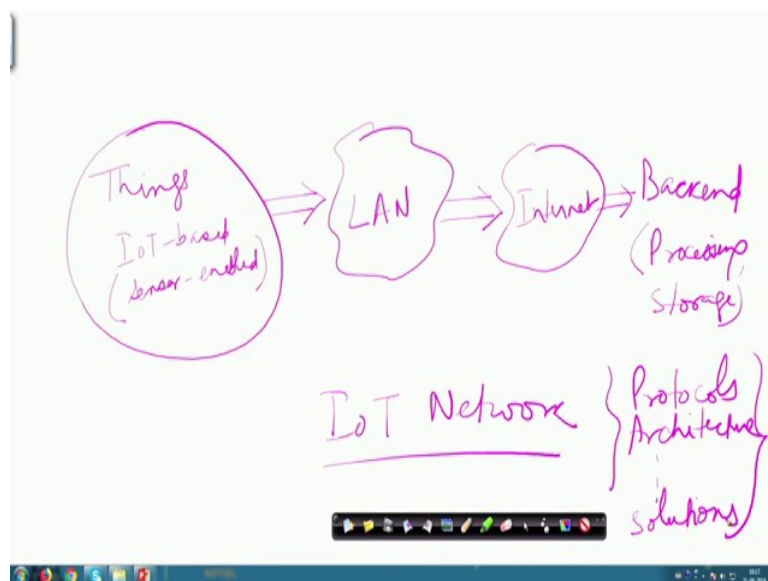
IPv6 talks about header compression encapsulation, these in order to allow the IPv6 packets from the network layer to be transmitted over IEEE 802.15.4 based networks. ROLL is a new kind of routing protocol that can be used that can be used for IoT-based applications.

Constrained RESTful Environment extends the integration of IoT devices from networks to the service level. And this is very essential, it is a important thing, service level; typically about the networks, collecting data from these networks in the context of IoT. CoRE is very crucial and an attraction in the IoT community.

(Refer Slide Time: 15:32)



(Refer Slide Time: 16:02)



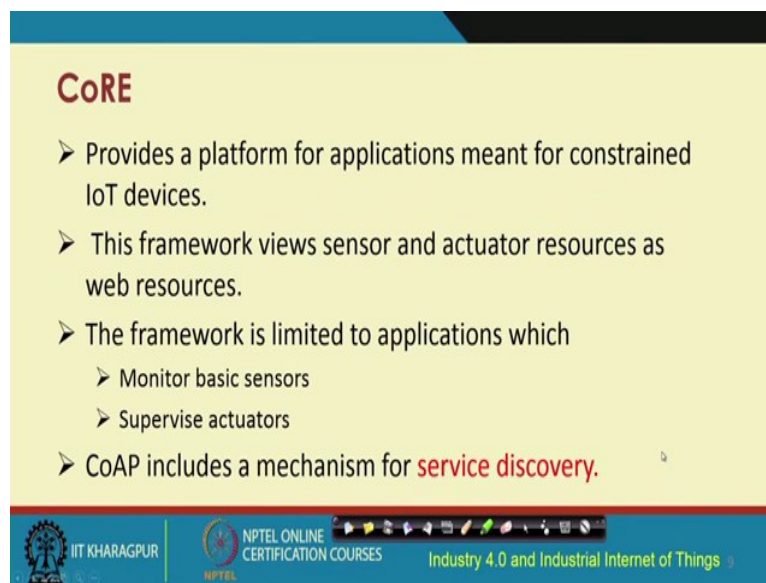
We have different IoT devices, which are the things. And these things are sensor enabled, sensor based, these are IoT-based.

IoT-based things are sensor enabled; this data are collected from these things, which are fitted with different sensors, these will transmit that collected data through something like a local area network; data further through the internet to the back end. The back end will would have all kinds of processors like servers; you will have storage devices including cloud etc. In the modern context; cloud-based services for processing storage.

This is the network and the corresponding protocols, architecture, and other aspects of solutions that we need to understand in considerable detail. So, here in this lecture we are simply introducing you about the overall concept of the networking aspects.

There are different IETF initiatives on supporting IoT over existing internet. Let us talk about the CoRE, which is Constrained RESTful Environments. REST is an acronym.

(Refer Slide Time: 18:57)



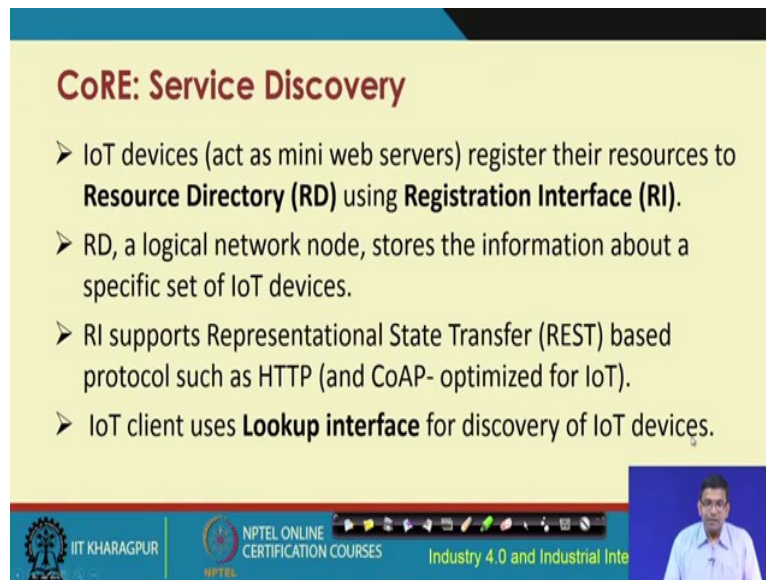
CoRE

- Provides a platform for applications meant for constrained IoT devices.
- This framework views sensor and actuator resources as web resources.
- The framework is limited to applications which
 - Monitor basic sensors
 - Supervise actuators
- CoAP includes a mechanism for **service discovery**.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

CoRE provides a platform for applications meant for constrained IoT devices and useful for IoT environments. This framework views sensors and actuator resources and web resources. The framework is limited to applications, which monitor basic sensors and supervise the actuators. CoAP includes a mechanism for service discovery and this service discovery makes it very interesting.

(Refer Slide Time: 19:30)



CoRE: Service Discovery

- IoT devices (act as mini web servers) register their resources to **Resource Directory (RD)** using **Registration Interface (RI)**.
- RD, a logical network node, stores the information about a specific set of IoT devices.
- RI supports Representational State Transfer (REST) based protocol such as HTTP (and CoAP- optimized for IoT).
- IoT client uses **Lookup interface** for discovery of IoT devices.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Inte

NPTEL

Video inset showing a speaker.

CoRE devices are mini web servers that register their resources to the resource directory and registration interface.

Resource directory is a logical network node that stores the information about a specific set of IoT devices. In any logical IoT node storing the information about a set of IoT devices. The registration interface, on the other hand, supports the REST-based protocol. The full form of REST architecture is REpresentational State Transfer architecture which support protocols such as http for the existing internet. For IoT, the equivalent of REST which is the CoAP; we will talk about in a little bit, further detail.

IoT client uses the lookup interface for discovery of IoT devices. Now everything is fine network has been built, but then whether the network is able to offer the quality of service guarantees or at least some acceptable levels of quality of service.

(Refer Slide Time: 20:54)

IoT Network QoS

- Quality-of-service (QoS) of IoT network is the ability to guarantee intended service to IoT applications through controlling the heterogeneous traffic generated by IoT devices.
- QoS policies for IoT Network includes
 - Resource utilization
 - Data timeliness
 - Data availability
 - Data delivery

Source: [Rayes, A., & Salam, S. \(2016\), "Internet of Things from hype to reality: the road to digitization", Springer.](#)

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

Quality of service of IoT network talks about offering different surfaces to the IoT applications through controlling the heterogeneous traffic generated by IoT devices.

QoS policies for IoT networks includes resource utilization, data timeliness, data availability, and data delivery. These are the 4 different attributes which are of prime consideration, in the context of QoS and ensuring QoS for IoT networks.

(Refer Slide Time: 21:39)

Resource utilization

- Requires control on the storage and bandwidth for data reception and transmission.
- QoS policies for resource utilization:
 - **Resource limit policy**
 - Controls the amount of message buffering
 - Useful for memory constrained IoT devices
 - **Time filter policy**
 - Controls the data sampling rate (interarrival time) to avoid buffer overflow
 - Controls network bandwidth, memory, and processing power

Source: [Rayes, A., & Salam, S. \(2016\), "Internet of Things from hype to reality: the road to digitization", Springer.](#)

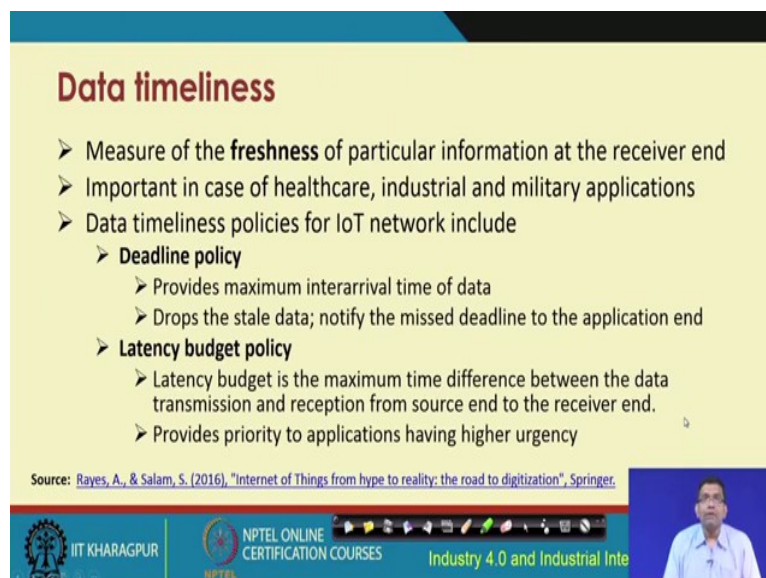
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Inte

Resource utilization is the first among the 4. It talks about the concept of control on the storage and bandwidth for data reception and transmission.

Resources in the context of networks mean different things such as storage, bandwidth etc. The control over these resources such as storage and bandwidth for reception and transmission is something that has to be considered as a QoS criterion.

QoS policies for resource utilization include resource limit policy, which controls the amount of message buffering and this is useful for memory constraint IoT devices. The second one is the QoS policy for resource utilization is time filter policy, which controls the data sampling rate and talks about the inter arrival time to avoid buffer overflow. These talks about the control over the network bandwidth memory and processing power.

(Refer Slide Time: 22:49)



Data timeliness

- Measure of the **freshness** of particular information at the receiver end
- Important in case of healthcare, industrial and military applications
- Data timeliness policies for IoT network include
 - **Deadline policy**
 - Provides maximum interarrival time of data
 - Drops the stale data; notify the missed deadline to the application end
 - **Latency budget policy**
 - Latency budget is the maximum time difference between the data transmission and reception from source end to the receiver end.
 - Provides priority to applications having higher urgency

Source: Rayes, A., & Salam, S. (2016). "Internet of Things from hype to reality: the road to digitization", Springer.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Inte

Timeliness the second attribute is the measurement of the freshness of a particular information; when it is received at the receiver end. From the source, the data that is sensed is sent at the receiver it is received, but then when it is received at the receiver, how much fresh that data is? And this is a very important consideration particularly for applications, where safety criticality, where there is real time requirements.

For example, healthcare the patient having heart attack. QoS criterion measure whether the data that is received at the receiver end. May be somebody having a heart attack; the packet containing that information whether that is fresh enough, whether the data has been received timely or not. This is a very important consideration in many of these applications.

Data timeliness policies for IoT networks include the deadline policy; that means, the maximum inter arrival time of data; how much is the maximum inter arrival time? This is a very important policy reconsideration. The second policy consideration is the latency budget policy consideration; which is the maximum time difference between the data transmission and reception from source end to the receiver end. So, these are the two different considerations for data timeliness.

(Refer Slide Time: 24:24)

Data availability

- Measure of the amount of valid data provided by the sender/producer to receiver/consumer
- QoS policies for data availability in IoT network include
 - **Durability policy**
 - Controls the degree of data persistence transmitted by the sender
 - Data persistence ensures the availability of the data to the receiver even after sender is unavailable
 - **Lifespan policy**
 - Controls the duration for which transmitted data is valid
 - **History policy**
 - Controls the number of previous data instances available for the receiver.²

Source: Rayes, A., & Salam, S. (2016). "Internet of Things from hype to reality: the road to digitization", Springer.

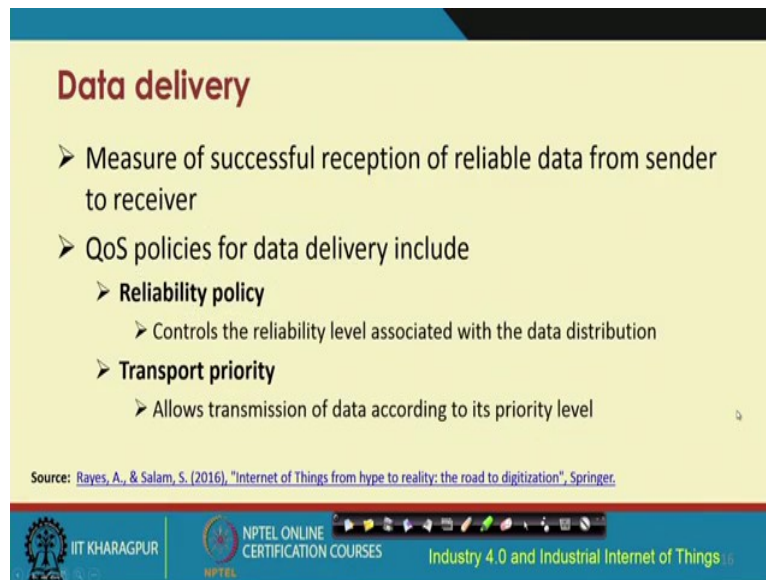
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Inte

The next attribute is the data availability, as this name suggests, is a measurement of the amount of valid data, provided by the sender or the producer to the receiver or the consumer. QoS policies for data availability in IoT networks include durability policy, life span policy, and history policy. Durability as this English term suggests; is the control of the degree of data persistence transmitted by the sender.

Data persistence is important; that means, ensuring the availability of the data to the receiver even after the sender is unavailable. The persistence of the data at the receiver is a very important durability policy consideration. Lifespan policy talks about the control over the duration for which the transmitted data will be valid. How much the data that has been sensed and is being circulated through the network, how much time it is going to survive, how much time it is going to live? This is a lifespan policy.

History policy is about controlling the number of previous data instances available to the data. In the history of the data, how many such instances are available to the receiver.

(Refer Slide Time: 25:43)



Data delivery

- Measure of successful reception of reliable data from sender to receiver
- QoS policies for data delivery include
 - **Reliability policy**
 - Controls the reliability level associated with the data distribution
 - **Transport priority**
 - Allows transmission of data according to its priority level

Source: Rayes, A., & Salam, S. (2016), "Internet of Things from hype to reality: the road to digitization", Springer.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

Data delivery is the last one, which measures successful reception of reliable data, from the sender to the receiver. QoS policies for data delivery are the reliability policy, which talks about the control of the reliability level associated with the data distribution and the transport priority. This allows transmission of data according to its priority level.

With this we come to an end of the first part of IoT networks. We will continue with the different other aspects of networking in IoT. And before we talk about those things, in detail, there are a few other issues that also need to be considered and that is what we are going to talk about in the next lecture.

Thank you.