Om Sakthi

Adhiparasakthi Engineering College
Melmaruvathur – 603319

Department of Computer Applications

MC4302 – INTERNET OF THINGS

UNIT - IV

UNIT IV - INTERNET OF THINGS PRIVACY, SECURITY AND GOVERNANCE

Introduction, Overview of Governance, Privacy and Security Issues, Contribution from FP7 Projects, Security, Privacy and Trust in IoT-Data-Platforms for Smart Cities, First Steps Towards a Secure Platform, Smartie Approach. Data Aggregation for the IoT in Smart Cities, Security

4.1 Introduction Internet of Things Privacy, Security and Governance:

- Trust, privacy and governance aspects of IoT rely for the most part upon security .
- Security in its broadest definitions includes health andwellbeing as well as other forms of protection.
- These aspects need to be viewed from the perspectives ofthe majority if not all the principle stakeholder groups andextended to include the relevant influencing andinfluenced elements of the general environment

Overview of governance:

1.The European Research Cluster on the Internet of Things has created a number of activity chains to favour close cooperation between the projects addressing IoT topics and to form an are a for ***exchange of ideas and open dialog on important research challenges***.

2.The activity chains are defined as work streams that group together partners or specific participants from partners around well defined technical activities that will result into at least one output or delivery that will be used in addressing the IERC objectives.

3.IERC Activity Chain 05 is a ***cross-project activity focused on making a valued contribution to IoT privacy, security*** and governance among the EC funded research projects in the area of Internet of Things.

4.“***Privacy, security and competition have been identified as the main issues related to IOT Governance*****.**

5.Overall, the main objective of the Activity Chain 05 is ***to identify research challenges and topics,*** which could make IoT more secure for users (i.e. citizen, business and government), to guarantee the privacy of users and support the confident, successful and trusted development of the IoT market.

6.In comparison to IoT initiatives in Europe or at a global level (e.g., IGF), ***Activity Chain 05 does not define government policies but focuses upon research***

Security issues in IoT

The Internet of Things (IoT) poses a number of security risks because of the large number of connected devices and the amount of personal and sensitive data they collect and transmit. Some of the main security issues in IoT include:

- ***Device vulnerabilities:*** Many IoT devices have poor security practices, such as using hard-coded or weak passwords, and lack of regular software updates, which make them easy to hack or compromise.
- ***Lack of encryption:*** Many IoT devices do not encrypt the data they transmit, making it easy for malicious actors to intercept and steal personal information.
- ***Network vulnerabilities:*** IoT devices often connect to a network, whether it be a local network or the internet. These networks can also be exploited by attackers to gain access to connected devices, steal data or launch cyber attacks
- ***Distributed denial of service (DDoS) attacks:*** IoT devices can be used to launch DDoS attacks, which flood a website or network with traffic, making it unavailable to users.
- ***Insufficient authentication:*** Many IoT devices lack proper authentication mechanisms

4.2 Contribution for FP7:

The FP7 (Seventh Framework Programme for Research and Technological Development) was a funding program established by the European Union (EU) that ran from 2007 to 2013, with the goal of supporting research and innovation in a wide range of areas, including the Internet of Things (IoT). During the duration of the program, a number of FP7 projects were launched with the goal of advancing the state of the art in IoT research and development. Some of the key contributions of these projects include:

- ***Development of new technologies:*** FP7 projects supported the development of new technologies for IoT, such as wireless sensor networks, low-power electronics, and machine learning.
- ***Standardization:*** FP7 projects contributed to the standardization of IoT technologies, such as the development of common communication protocols, data formats, and security standards.
- ***Test-beds and pilots:*** FP7 projects established test-beds and pilots for IoT technologies, allowing for the experimentation and validation of new technologies in real-world settings.
- ***Interoperability and scalability:*** FP7 projects aimed at promoting interoperability and scalability across different IoT domains and technologies, such as building automation, transportation, and healthcare, and across different regions of Europe.
- ***Security and Privacy :*** FP7 projects tried to address security and privacy issues in IoT, by studying the potential threats and vulnerabilities in IoT systems and developing new security and privacy mechanisms to protect the data of IoT systems.
- ***Field testing:*** many of the projects were field-testing the developed technologies, this helped to get real-world feedback and validate the solutions, hence making them more reliable and robust.

Overall, the FP7 program played a key role in supporting IoT research and development in Europe, and many of the technologies and standards developed through FP7 projects are still in use today.

1. FP7 iCore Access Framework (iCore Contribution)
2. IoT@Work Capability Based Access Control System(IoT@Work Contribution)
3. GAMBAS Adaptive Middleware (GAMBAS Contribution)
4. IoT-A Architecture (IoT-A Contribution)
5. Governance, Security and Privacy in the Butler Project (Butler Contribution)

Security, privacy and trust of IOT- Data platforms for smart cities:

Security, privacy, and trust are critical issues in the implementation of IoT data platforms for smart cities. These issues are interrelated and must be addressed together to ensure the safe and secure operation of smart cities.

- ***Security:*** IoT data platforms for smart cities are vulnerable to cyber attacks, such as data breaches, denial of service attacks, and unauthorized access. Security measures such as encryption, secure communications protocols, and network segmentation can help protect against these types of attacks.
- ***Privacy:*** Smart cities generate a large amount of personal data, and it's important to ensure that this data is protected from unauthorized access, use, or disclosure. Measures such as

data minimization, anonymization, and secure data storage can help protect personal data.

- ***Trust:*** The public needs to trust that their personal data is being used responsibly and that the systems in place can protect the data from unauthorized access. Transparency, clear communication, and building trust through reputation systems are ways to gain and retain the trust of the public.
- ***Federated Learning***: In order to preserve data privacy, techniques such as federated learning can be used to aggregate data from different smart city devices while keeping the data on the device, allowing for better privacy protection.
- ***Compliance:*** Smart City platforms must comply with various regulations such as GDPR, HIPAA, and other local regulations. Ensuring compliance with these regulations is essential to preserving privacy, security and build trust.
- ***Governance:*** clear governance structures need to be in place to ensure that the data is used responsibly, and that security and privacy policies are adhered to. This can include data access controls, incident response plans, and regular security audits.

In summary, Security, Privacy and Trust are essential elements of IoT-Data-Platforms for Smart Cities, it's important to take necessary measures, to ensure the safe and secure operation of the smart city, promote trust and ensure compliance with regulations to protect personal data.

One of the main aims of Smart City technologies is to provide different optimization mechanisms for different aspects of data management.

- Data is gathered from various sources owned by different administrative domains. Noteworthy parts are data from public and private transportation providers, data from mobile users, captured for instance with their smart phones, surveillance data and videos from private and public organisations and a vast amount of sensors and meters, attached to machines and infrastructures, distributed throughout the city.
- All this information is stored in a variety of different places, for instance it can remain locally in the sensors or company internal databases, in social networks, in data storage located in private data centres or even in a public cloud storage service.
- Also actuation decisions can be taken in a coordinated way between multiple control centres or data providers. Hence it is clear that there is a need of an information sharing platform in which data flows from various sources and from different Security, Privacy and Trust in Iot-Data-Platforms for Smart Cities 227 Architectural components.
- All parties involved in the overall systems such as sensors and actuators, end users, data owners but also service providers need strong mechanisms for reliability and trust.. For instance, a user might be willing to share location information with family and friends and make the information available in aggregated form for improvement of the public transport.

However, several challenges need to be overcome to make this possible. Creating a platform for sharing IoT-type of data is per se a huge challenge.

Risks to a Smart City IoT Platform

We predict that smart city data will eventually be stored in the cloud and employ cloud computing techniques, due to the high scalability of resources and computing performance and reduced cost in maintenance and operation.

1. Cybersecurity Threats

Smart city IoT platforms are prime targets for cybercriminals due to the vast amount of data they collect and the critical infrastructure they support. Potential risks include:

- **Data Breaches**: Unauthorized access to sensitive data, including personal information of citizens and operational data of city services, can lead to identity theft and loss of trust in public institutions.
- **Denial-of-Service Attacks**: Attackers can overwhelm city services by flooding the network with traffic, disrupting essential services like traffic management, public safety, and utilities.
- **Ransomware**: Malicious software can encrypt critical systems, demanding payment for their release, effectively paralyzing city operations.

2. Data Privacy Concerns

The extensive data collection inherent in Smart City initiatives can raise significant privacy issues:

- **Surveillance and Monitoring**: Continuous data collection through cameras, sensors, and mobile applications can create a perception of surveillance, leading to public backlash.
- **Consent and Transparency**: Citizens may not fully understand how their data is being used, leading to concerns over consent and the ethical use of information.
- **Data Misuse**: Without strict governance, collected data could be misused by third parties for marketing or other unintended purposes.

3. Interoperability Challenges

Smart cities often utilize a multitude of devices and platforms, which can lead to interoperability issues:

- **Compatibility**: Devices from different manufacturers may not communicate effectively, resulting in inefficiencies and gaps in service delivery.
- **Standardization**: The lack of universal standards for IoT devices can hinder integration efforts, making it difficult to implement cohesive solutions across the city.

4. Dependence on Connectivity

The functionality of a Smart City relies heavily on stable and robust connectivity:

- **Network Reliability**: Interruptions in connectivity can severely disrupt services such as public transportation systems, emergency response, and environmental monitoring.
- **Infrastructure**: Aging or insufficient communication infrastructure can lead to outages and impact the performance of IoT systems.

5. Scalability Issues

As cities expand and more IoT devices are deployed, scalability becomes a critical concern:

- **Resource Management**: Scaling up requires effective management of both hardware and software resources, which can be challenging as complexity increases.
- **Performance Degradation**: An influx of new devices may strain existing systems, leading to slower response times and reduced overall performance.

6. Vendor Lock-In

Many Smart City solutions rely on specific vendors, which can lead to dependency risks:

- **Limited Flexibility**: Organizations may find it difficult to switch vendors or integrate new technologies, potentially stifling innovation.
- **Support and Maintenance Risks**: If a vendor fails to provide adequate support or goes out of business, the city could face significant challenges in maintaining its systems.

7. Infrastructure Vulnerabilities

Physical infrastructure that supports IoT platforms is also at risk:

- **Natural Disasters**: Events like floods, earthquakes, or severe storms can damage sensors and data collection points, disrupting city services.
- **Sabotage**: Deliberate attacks on physical infrastructure can cripple critical city functions, such as public safety and utilities.

8. Regulatory Compliance

Smart cities operate under a complex web of regulations:

- **Data Protection Laws**: Compliance with regulations like GDPR or local privacy laws can be challenging and may require significant resources to manage.
- **Operational Standards**: Adhering to various safety and operational standards across multiple jurisdictions can complicate deployment and management.

9. Public Acceptance

The success of Smart City initiatives hinges on public support:

- **Perception of Privacy Invasion**: Citizens may feel their privacy is being compromised, leading to resistance against certain technologies or initiatives.
- **Engagement and Communication**: Failure to effectively communicate the benefits and goals of IoT initiatives can lead to misunderstanding and mistrust.

10. Maintenance and Management

Ongoing maintenance is crucial for the reliability of IoT systems:

- **Obsolescence**: Rapid technological advancements can render devices outdated quickly, necessitating frequent upgrades.
- **Resource Allocation**: Limited budgets may lead to insufficient resources for regular maintenance, increasing vulnerability to failures.

11. Cost Overruns

The complexity of implementing Smart City projects often leads to unexpected costs:

- **Budget Constraints**: Overruns can occur due to unforeseen challenges in integration, maintenance, or compliance, potentially leading to project delays or cancellations.
- **Long-Term Sustainability**: Initial funding may not cover ongoing operational costs, jeopardizing the sustainability of the platform.

12. Technological Obsolescence

The fast pace of technological change can create risks for Smart City IoT platforms:

- **Rapid Innovation**: As new technologies emerge, existing systems may quickly become outdated, requiring continuous investment to remain relevant.
- **Legacy Systems**: Older technologies may lack the capabilities needed for effective integration with new IoT solutions, leading to increased complexity and costs.

Navigating the risks associated with a Smart City IoT platform requires a comprehensive strategy that includes robust cybersecurity measures, clear data governance policies, effective public engagement, and a commitment to ongoing maintenance and innovation. By proactively addressing these risks, cities can harness the full potential of IoT technologies to improve urban living while ensuring safety, privacy, and efficiency.

First Steps Towards a Secure Platform:

Past and current projects, such as UbiSec&Sense, SENSEI, WSAN4CIP provide already some solutions on which a platform as outlined above can build.

- We present in this section certain components, which can be used as building blocks, but also components that need further development to be suitable for the type of platform SMARTIE aims for.

1. Trust and Quality-of-Information in an Open Heterogeneous Network
2. Privacy-preserving Sharing of IoT Data
3. Minimal Disclosure
4. Secure Authentication and Access Control in Constrained Devices

To establish a secure platform, especially for IoT, there are several foundational steps that organizations can take. Here’s a structured guide to help you get started:

1. Conduct a Risk Assessment

- **Identify Assets**: Make a comprehensive inventory of all devices, software, and data that will be part of the platform.
- **Assess Vulnerabilities**: Evaluate potential weaknesses in each component, considering both hardware and software aspects.
- **Determine Impact**: Analyze the potential consequences of security breaches on operations, data integrity, and user privacy.

2. Develop a Security Strategy

- **Create Security Policies**: Formulate policies that address data protection, user access, and acceptable use of the platform.
- **Adopt Security Frameworks**: Use established frameworks (e.g., NIST, ISO/IEC 27001) to guide security practices and ensure a systematic approach.

3. Implement Strong Authentication and Access Control

- **Multi-Factor Authentication (MFA)**: Require multiple forms of verification for users accessing the platform to enhance security.
- **Role-Based Access Control (RBAC)**: Assign permissions based on user roles, ensuring that individuals can only access information relevant to their functions.

4. Ensure Data Encryption

- **Encrypt Data in Transit**: Use secure protocols (like TLS) to protect data transmitted over networks.
- **Encrypt Data at Rest**: Implement encryption for stored data to safeguard against unauthorized access.

5. Prioritize Device Security

- **Secure Configuration**: Configure devices securely by changing default settings and disabling unnecessary features.
- **Regular Firmware Updates**: Establish a process for promptly updating device firmware and software to mitigate known vulnerabilities.

6. Design for Scalability and Resilience

- **Modular Architecture**: Create a flexible architecture that allows for easy scaling and integration of new devices and services.
- **Redundancy**: Build redundancy into critical systems to ensure reliability in case of failures or security incidents.

7. Establish Monitoring and Incident Response Protocols

- **Continuous Monitoring**: Implement real-time monitoring of the platform to detect anomalies and potential threats.
- **Incident Response Plan**: Develop a clear plan for responding to security incidents, outlining steps for containment, investigation, and recovery.

8. Engage Stakeholders and Build Awareness

- **Stakeholder Collaboration**: Involve city officials, technology partners, and community representatives in discussions about security.
- **User Training**: Provide ongoing training on security best practices for users and staff to foster a culture of security awareness.

9. Adopt a Privacy-By-Design Approach

- **Data Minimization**: Collect only the necessary data for intended purposes, reducing the risk of exposure.
- **Transparency**: Clearly communicate data collection practices to users, ensuring informed consent and understanding.

10. Plan for Compliance and Legal Considerations

- **Understand Regulatory Requirements**: Familiarize yourself with relevant laws and regulations regarding data protection and cybersecurity.
- **Regular Compliance Audits**: Implement processes for periodic audits to ensure adherence to legal and regulatory standards.

By following these initial steps, organizations can establish a secure platform that protects sensitive data, ensures operational integrity, and fosters user trust. Continuous improvement and adaptation to new threats will be essential to maintaining security over time.

Smartie Approach:

SMARTIE will design and build a data-centring information sharing platform in which information will be accessed through an information service layer operating above heterogeneous network devices and data sources and provide services to diverse applications in a transparent manner. It is crucial for the

approach that all the layers involve appropriate mechanisms to protect the data already at the perception layer as well as at the layers on top of it. These mechanisms shall cooperate in order to provide a cross-layer holistic approach.

SMARTIE will focus on key innovations that strengthen security, privacy and trust at different IoT Layers as depicted in the following table:

IoT layers	Security requirements

Applications (Intelligent Transportation, Smart Energy, Public Safety, Utilities, Service Providers, etc.)	• Authentication, Authorisation, Assurance; • Privacy Protection and Policy Management; • Secure Computation; • Application-specific Data Minimisation; • Discovery of Information Sources
Information Services (In-network Data Processing, Data aggregation, Cloud Computing, etc.)	• Cryptographic Data Storage; • Protected Data Management and Handling (Search, Aggregation, Correlation, Computation);
Network (Networking infrastructure and Network-level protocols.)	• Communication & Connectivity Security; • Secure Sensor/Cloud Interaction; • Cross-domain Data Security Handling
Smart Objects (Sensors for data collection, Actuators)	• Data Format and Structures; • Trust Anchors and Attestation; • Access Control to Nodes • Lightweight Encryption

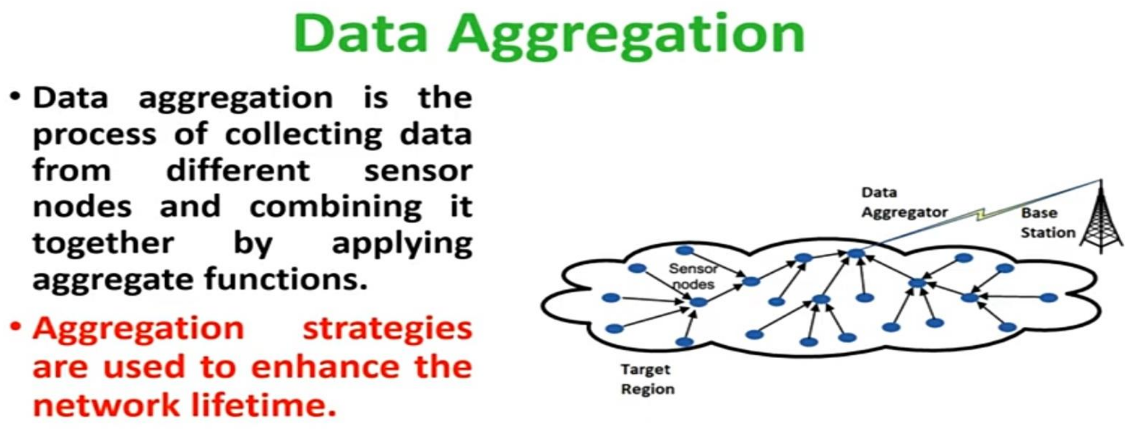
Adaptation and Deployment

- Smart Transportation
- Smart City Objectives
- Smart campus

Conclusion:

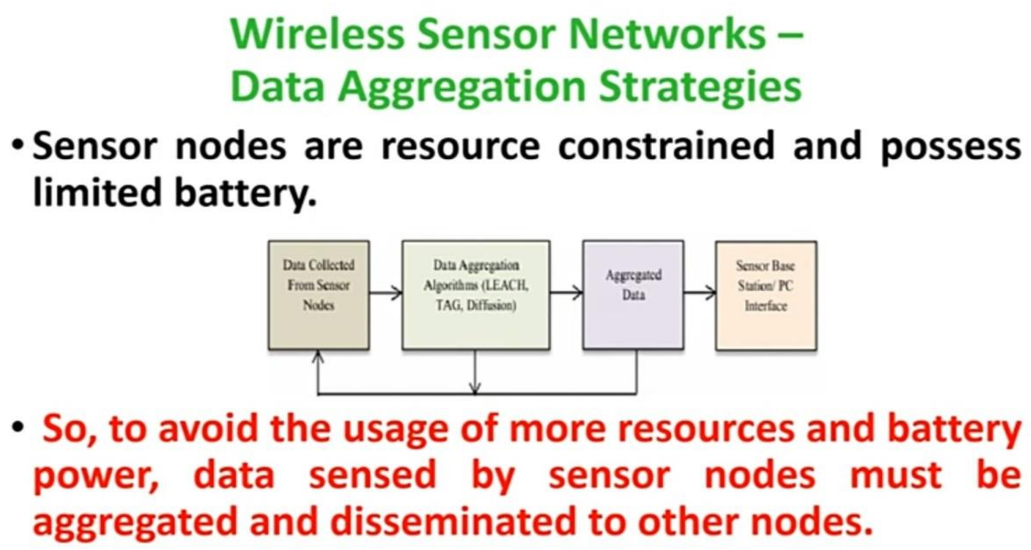
The Internet of the Future will be a cluster of heterogeneous current and future infrastructures (networks, services, data, virtual entities, etc.) and of usages with mainly decentralized security and trust functions. The emergence of sensing and actuating devices, the proliferation of user-generated content and nascent (Internet-only) services delivery create the need to address trust and security functions adequately.

Data Aggregation for the IoT in Smart Cities, Security:



Data Aggregation

- Data aggregation is the process of collecting data from different sensor nodes and combining it together by applying aggregate functions.
- Aggregation strategies are used to enhance the network lifetime.

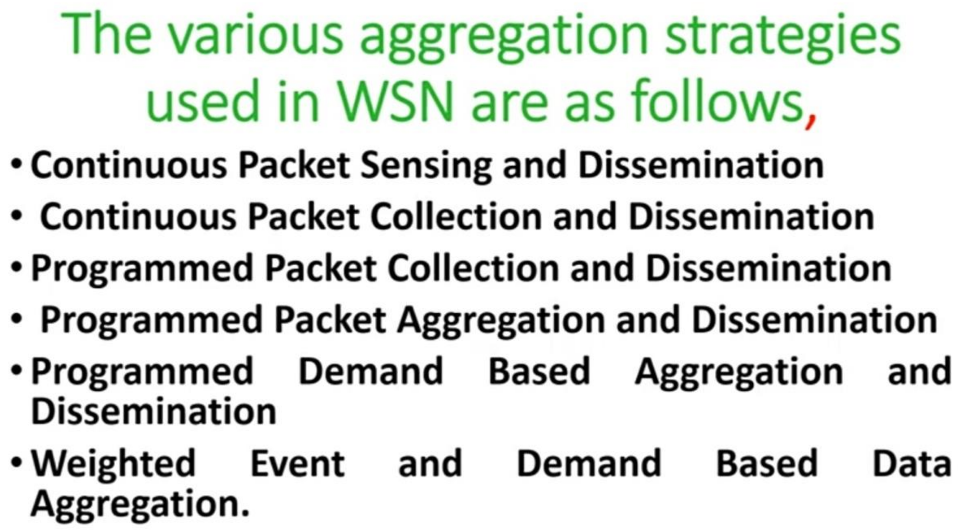


Wireless Sensor Networks – Data Aggregation Strategies

- Sensor nodes are resource constrained and possess limited battery.

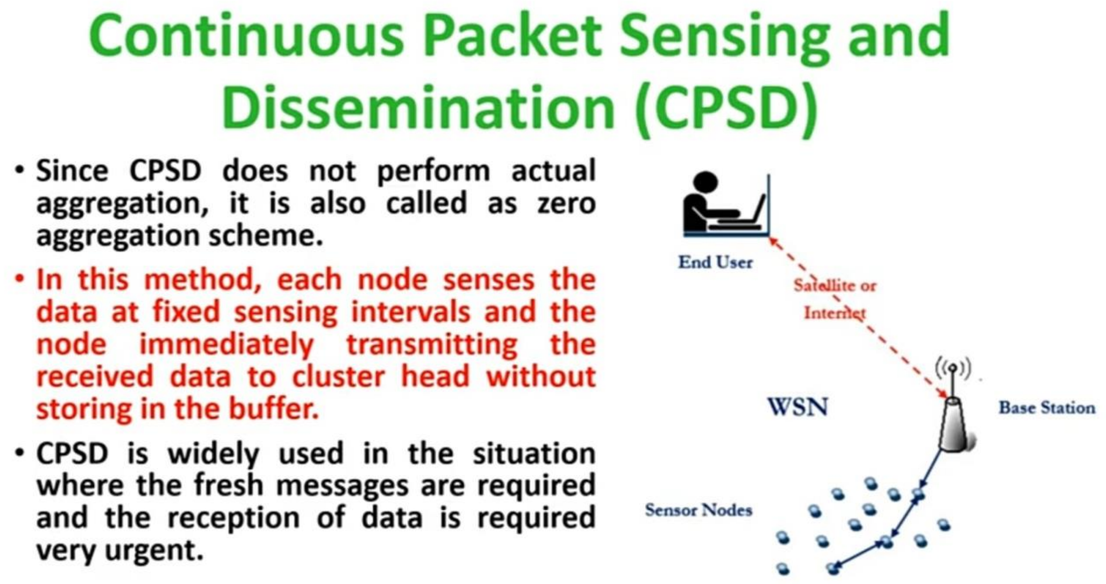
Data Collected From Sensor Nodes
Data Aggregation Algorithms (LEACH, TAG, Diffusion)
Aggregated Data
Sensor Base Station/ PC Interface

- So, to avoid the usage of more resources and battery power, data sensed by sensor nodes must be aggregated and disseminated to other nodes.



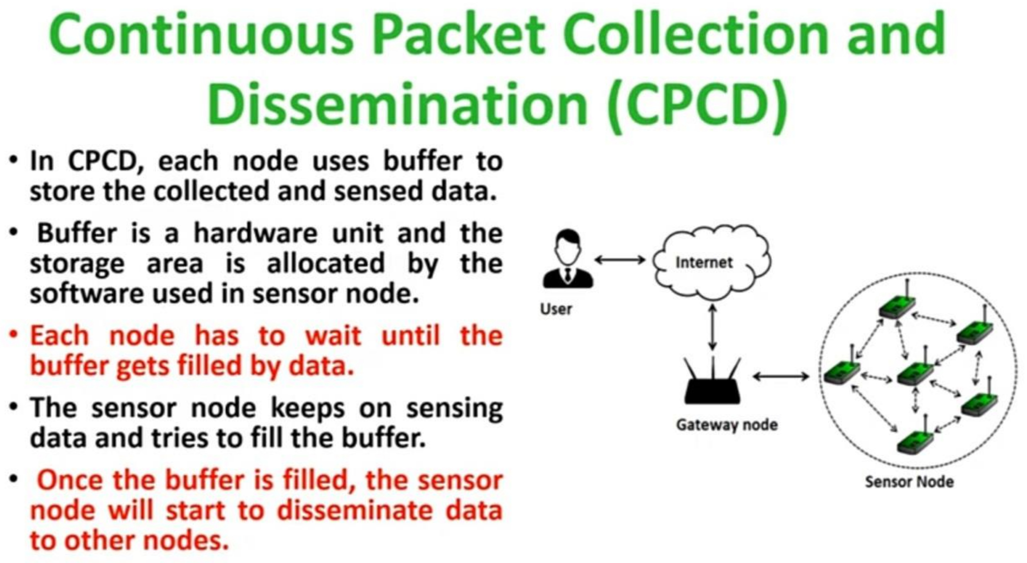
The various aggregation strategies used in WSN are as follows,

- Continuous Packet Sensing and Dissemination
- Continuous Packet Collection and Dissemination
- Programmed Packet Collection and Dissemination
- Programmed Packet Aggregation and Dissemination
- Programmed Demand Based Aggregation and Dissemination
- Weighted Event and Demand Based Data Aggregation.



Continuous Packet Sensing and Dissemination (CPSD)

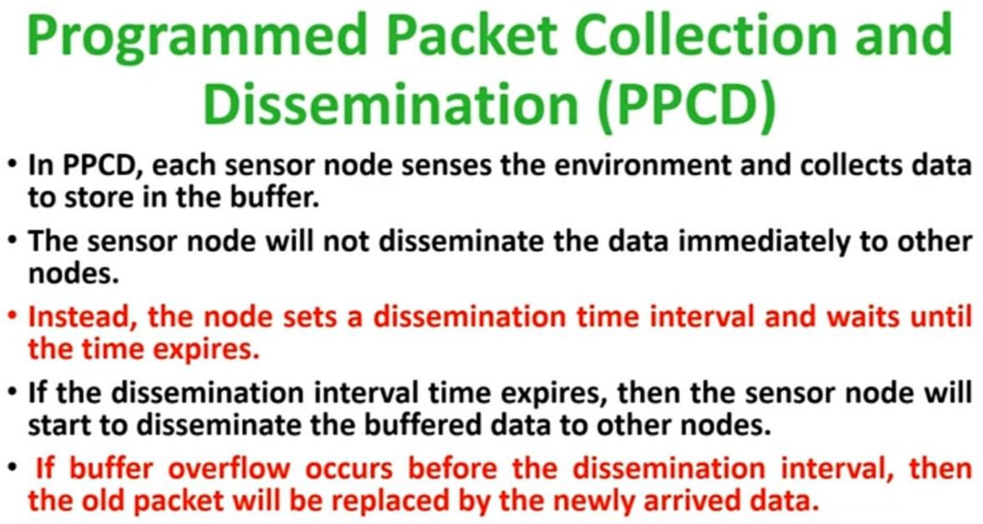
- Since CPSD does not perform actual aggregation, it is also called as zero aggregation scheme.
- In this method, each node senses the data at fixed sensing intervals and the node immediately transmitting the received data to cluster head without storing in the buffer.
- CPSD is widely used in the situation where the fresh messages are required and the reception of data is required very urgent.



Continuous Packet Collection and Dissemination (CPCD)

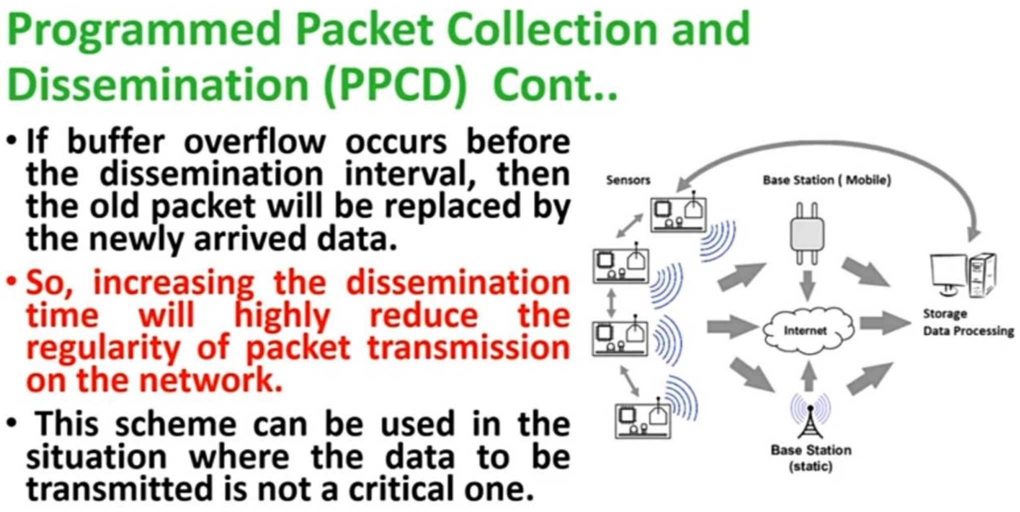
- In CPCD, each node uses buffer to store the collected and sensed data.
- Buffer is a hardware unit and the storage area is allocated by the software used in sensor node.
- Each node has to wait until the buffer gets filled by data.
- The sensor node keeps on sensing data and tries to fill the buffer.
- Once the buffer is filled, the sensor node will start to disseminate data to other nodes.

User
Internet
Gateway node
Sensor Node



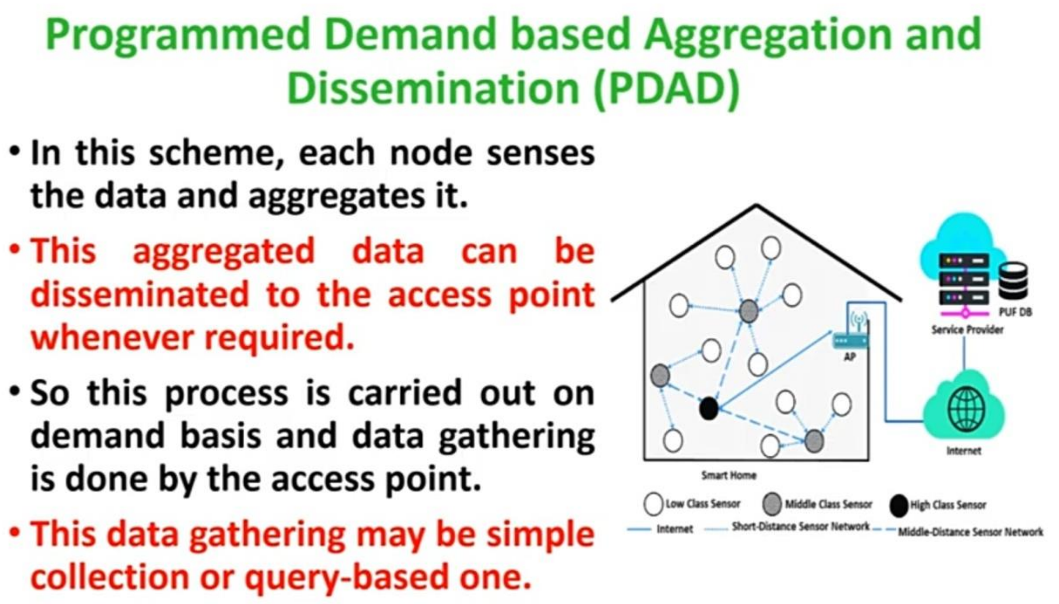
Programmed Packet Collection and Dissemination (PPCD)

- In PPCD, each sensor node senses the environment and collects data to store in the buffer.
- The sensor node will not disseminate the data immediately to other nodes.
- Instead, the node sets a dissemination time interval and waits until the time expires.
- If the dissemination interval time expires, then the sensor node will start to disseminate the buffered data to other nodes.
- If buffer overflow occurs before the dissemination interval, then the old packet will be replaced by the newly arrived data.



Programmed Packet Collection and Dissemination (PPCD) Cont..

- If buffer overflow occurs before the dissemination interval, then the old packet will be replaced by the newly arrived data.
- So, increasing the dissemination time will highly reduce the regularity of packet transmission on the network.
- This scheme can be used in the situation where the data to be transmitted is not a critical one.



Programmed Demand based Aggregation and Dissemination (PDAD)

- In this scheme, each node senses the data and aggregates it.
- This aggregated data can be disseminated to the access point whenever required.
- So this process is carried out on demand basis and data gathering is done by the access point.
- This data gathering may be simple collection or query-based one.

Text book: Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems by Dr. Ovidiu Vermesan,Dr. Peter Friess

Thank you...