# FIT5187-S1_2018 Lecture 11
# Future Generation of Mobile Networks and Devices

# Learning outcomes

1. Describe the integration of 5G heterogeneous mobile networks
2. Apply the software radio and software defined network to future mobile networks
3. Acquire data via heterogeneous IoT devices
4. Analyse the future generation of network security

# A framework for coexistence of Wifi and Lifi

## Reference:

[1] Moussa Ayyash, Hany Elgala, Abdallah Khreishah, Volker Jungnickel, Thomas Little, Sihua Shao, Michael Rahaim, Dominic Schulz, Jonas Hilt, and Ronald Freundes “Coexistence of WiFi and LiFi Toward 5G: Concepts, Opportunities, and Challenges.”

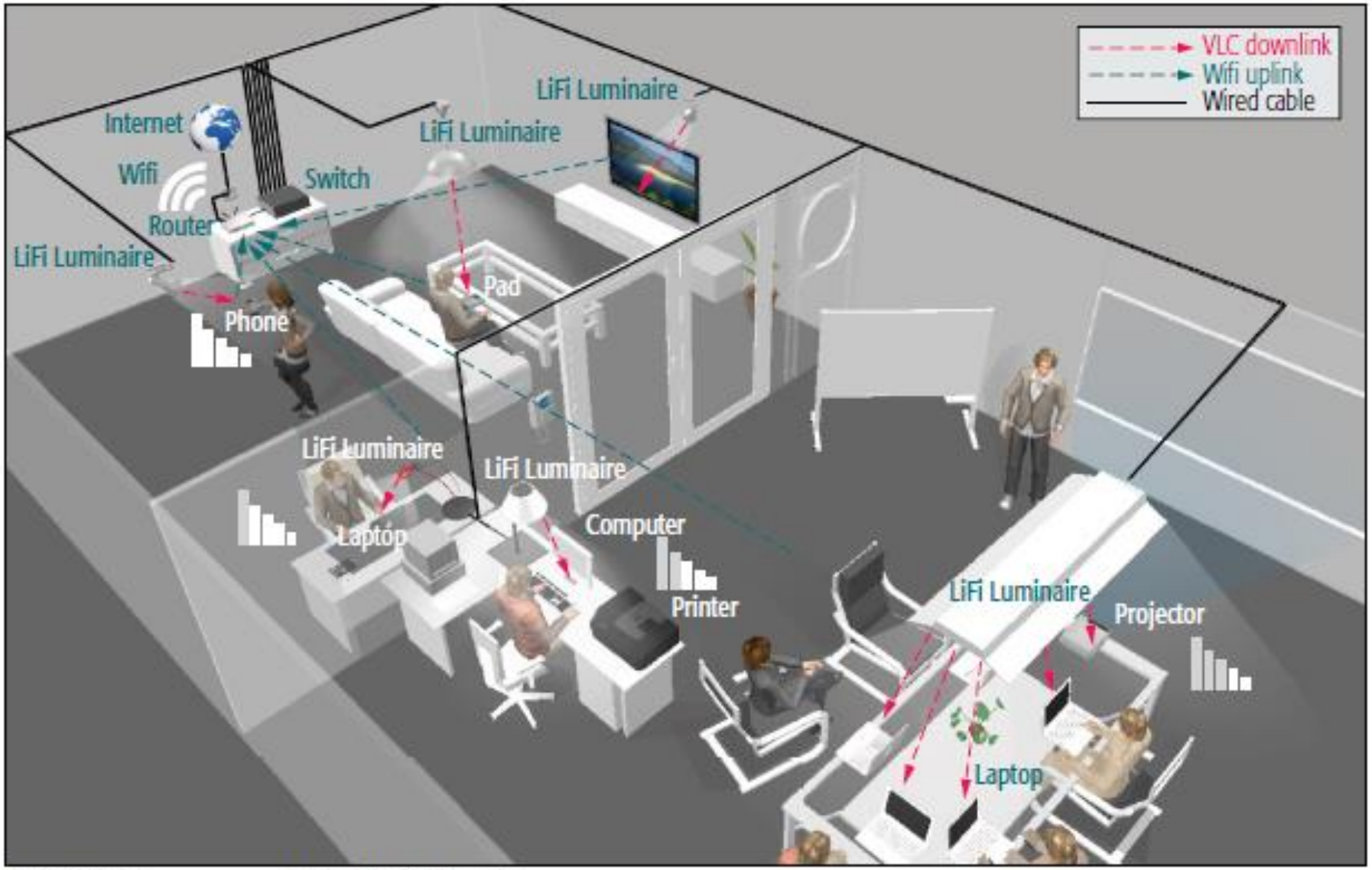



Figure 1. The proposed Li+WiFi HetNet.

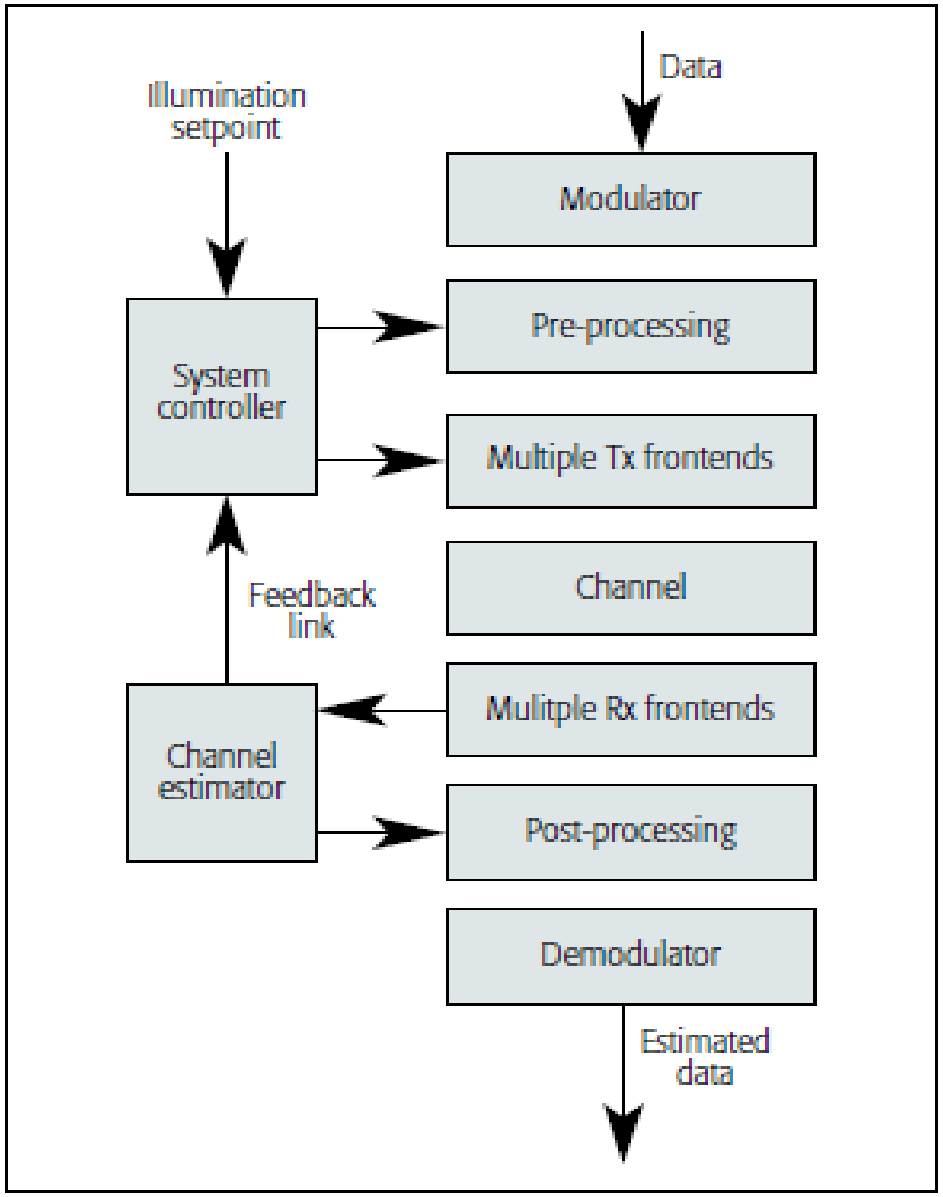



Figure 2. The SU-SVD-MIMO concept can be used to avoid interference and maintain target illumination. The SVD is used to decompose the MIMO channel into parallel SISO sub-channels, enabling interference-free spatial multiplexing. At the receiver, and after estimating the channel, the information needed to pre-process and post-process the signals at the transmitter and receiver, respectively, and the illumination set point (room brightness) is available on the feedback channel, to extract the parallel SISO channels.

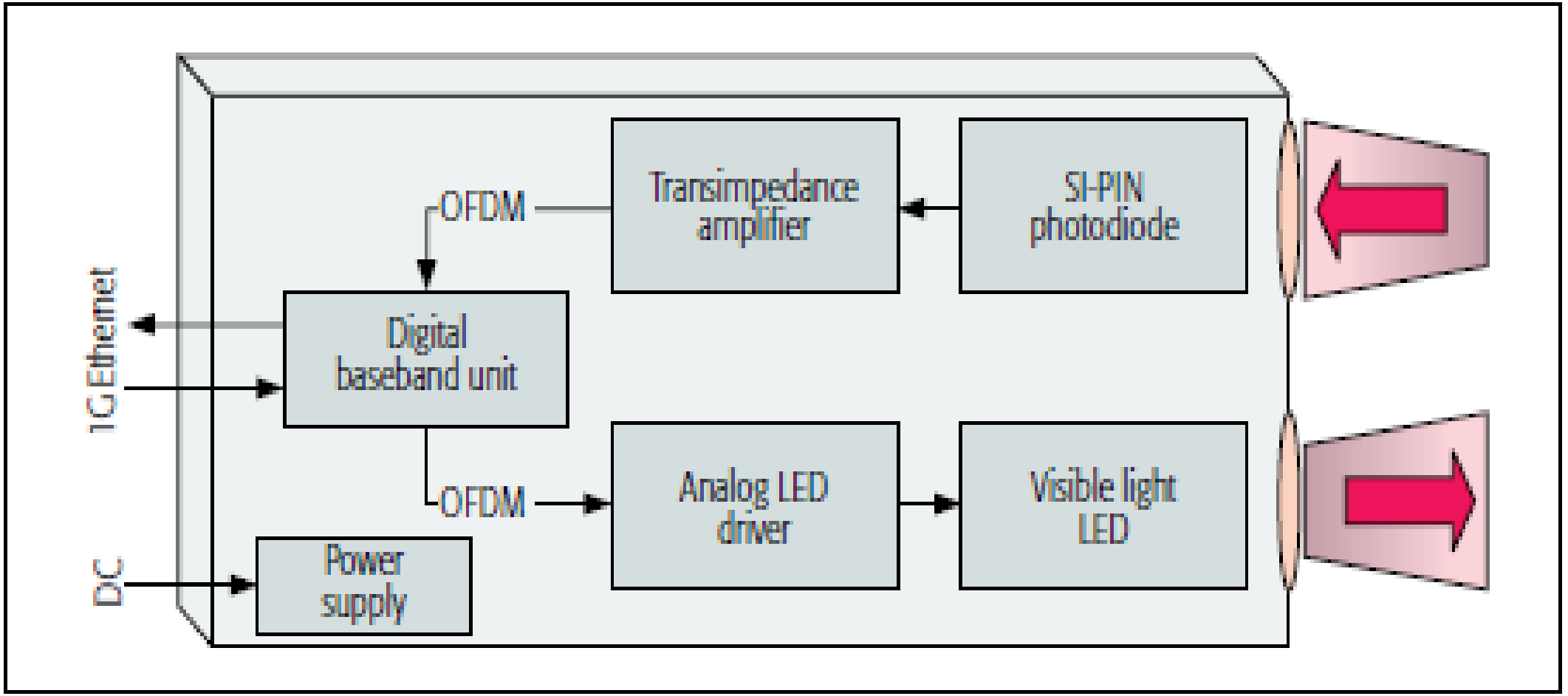



Figure 3. The LiFi transceivers.

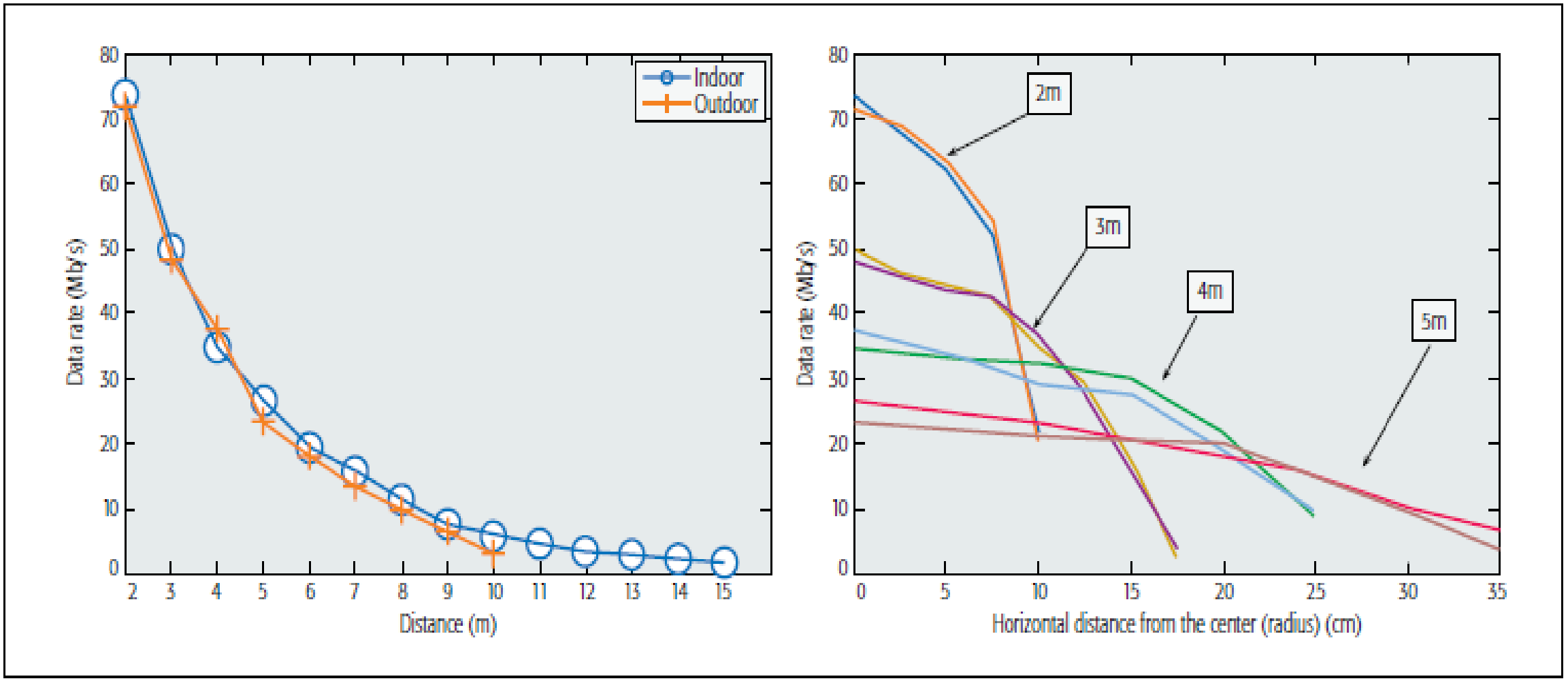



Figure 4. Vertical and horizontal distance between LiFi transceivers.

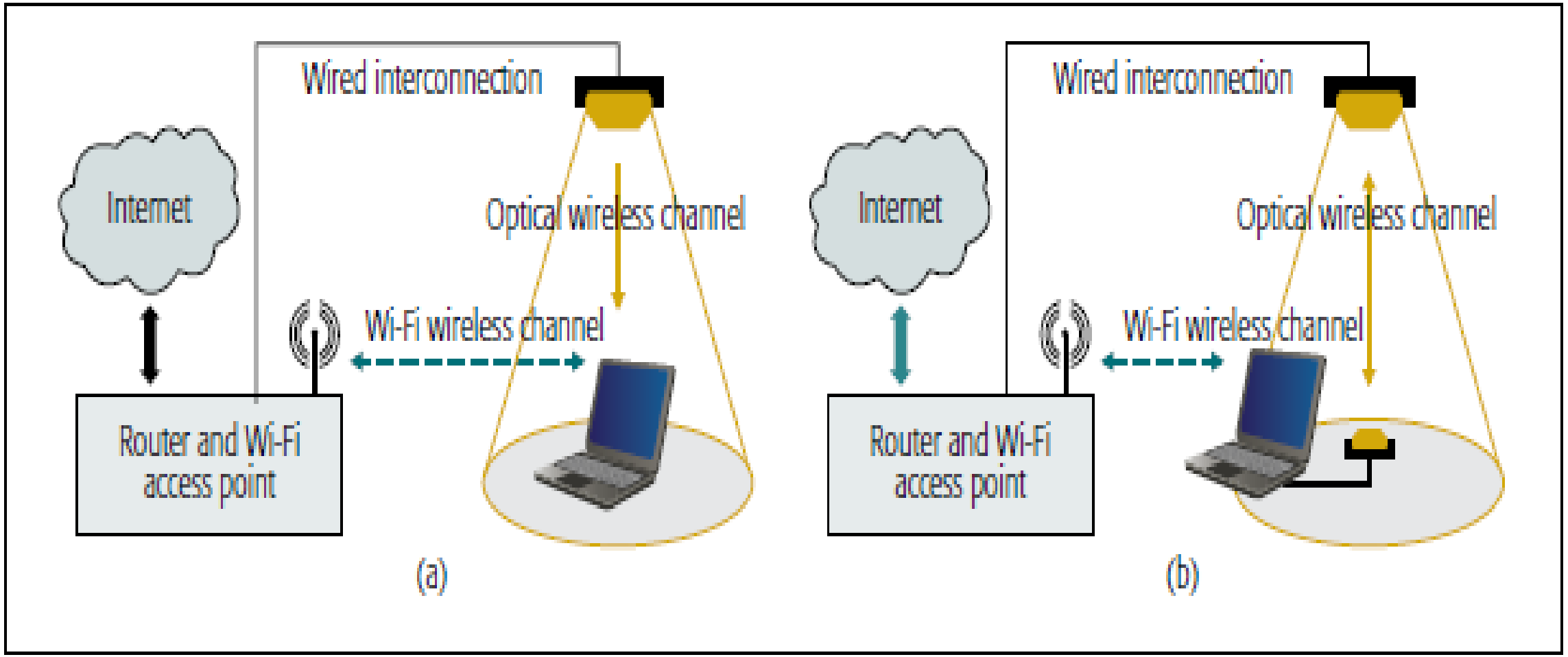



Figure 5. Configurations of the a) hybrid system, and b) the aggregated system.

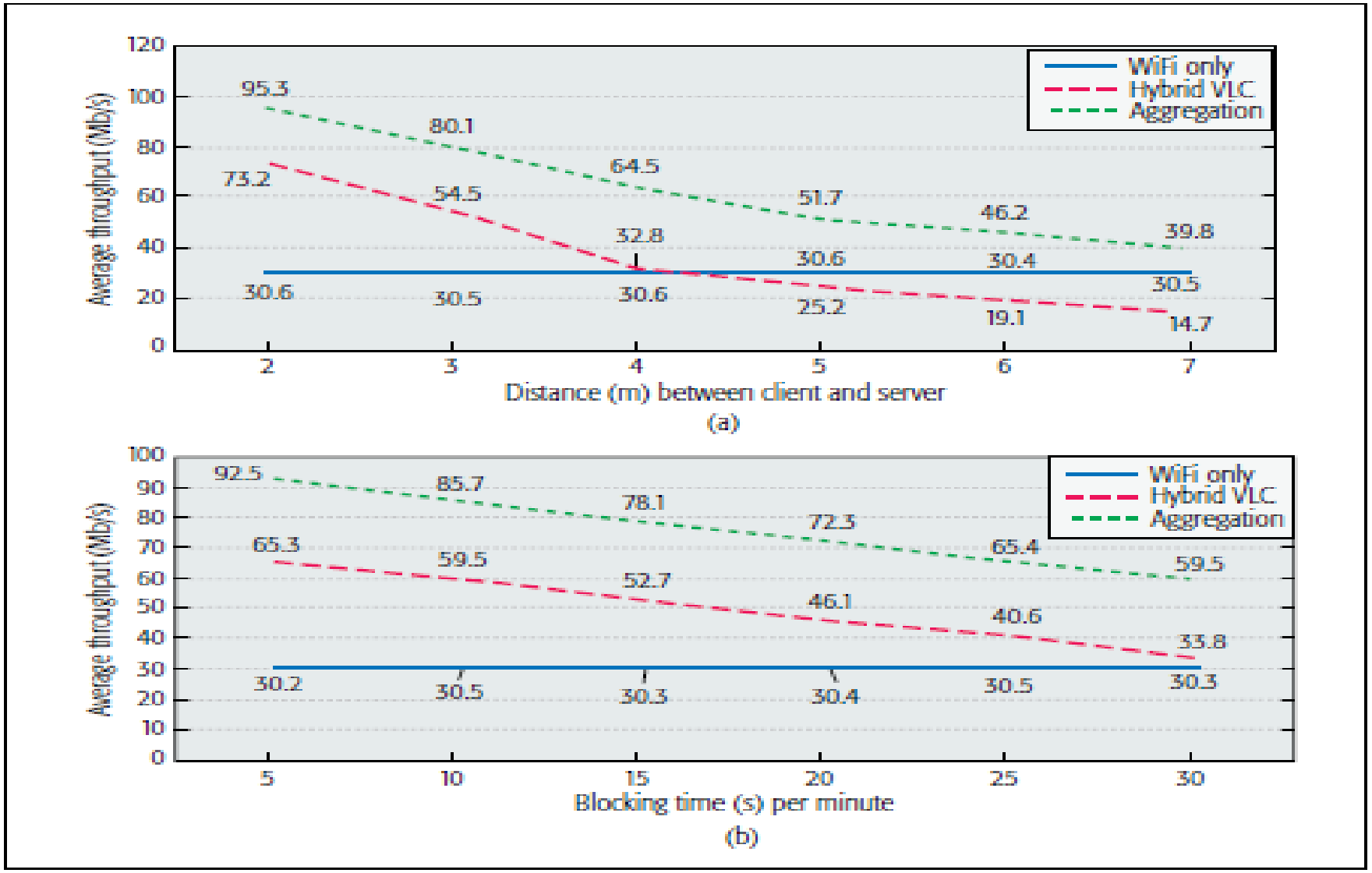



**Figure 6.** a) throughput vs. distance; b) throughput vs. blockage duration.

# Integration of SDN and SDR for 5G

Hsin-Hung Cho, Chin-Feng Lai, Timothy K. Shih, Han Chieh Chao, IEEE Access, vol. 2, 2014.

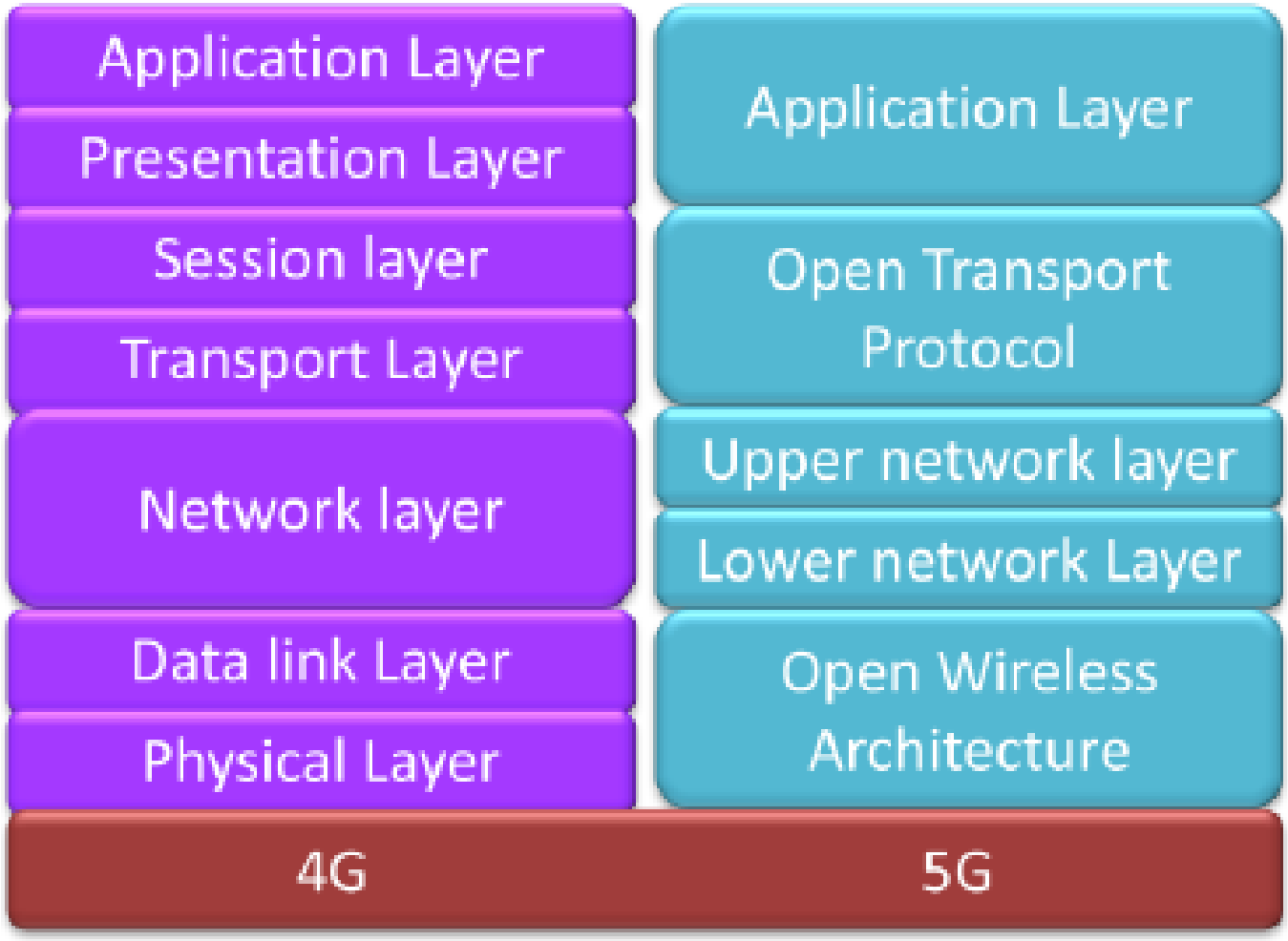



**FIGURE 1. The difference between 4G and 5G.**

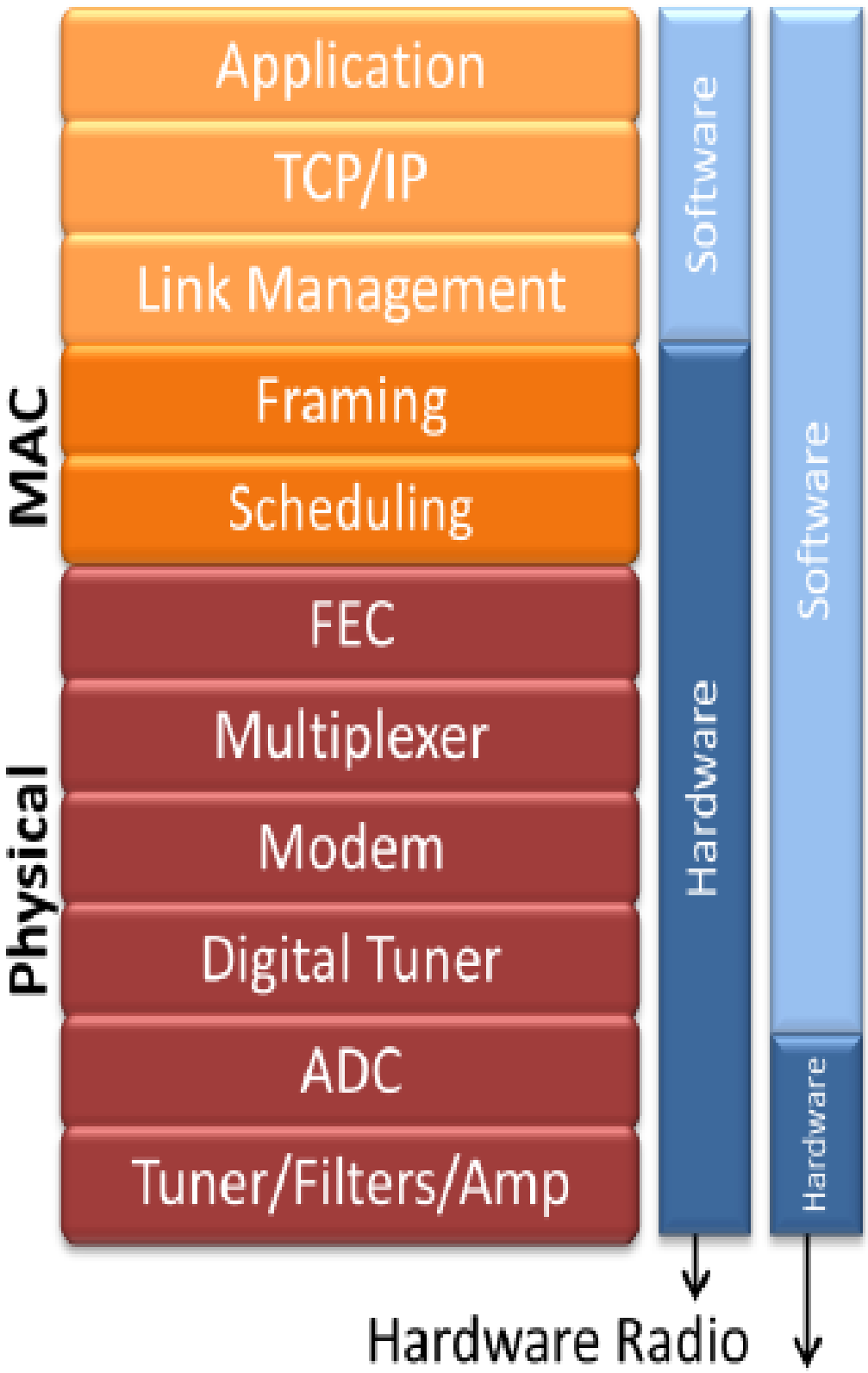



**FIGURE 2.** The software wireless support multi-layer control.

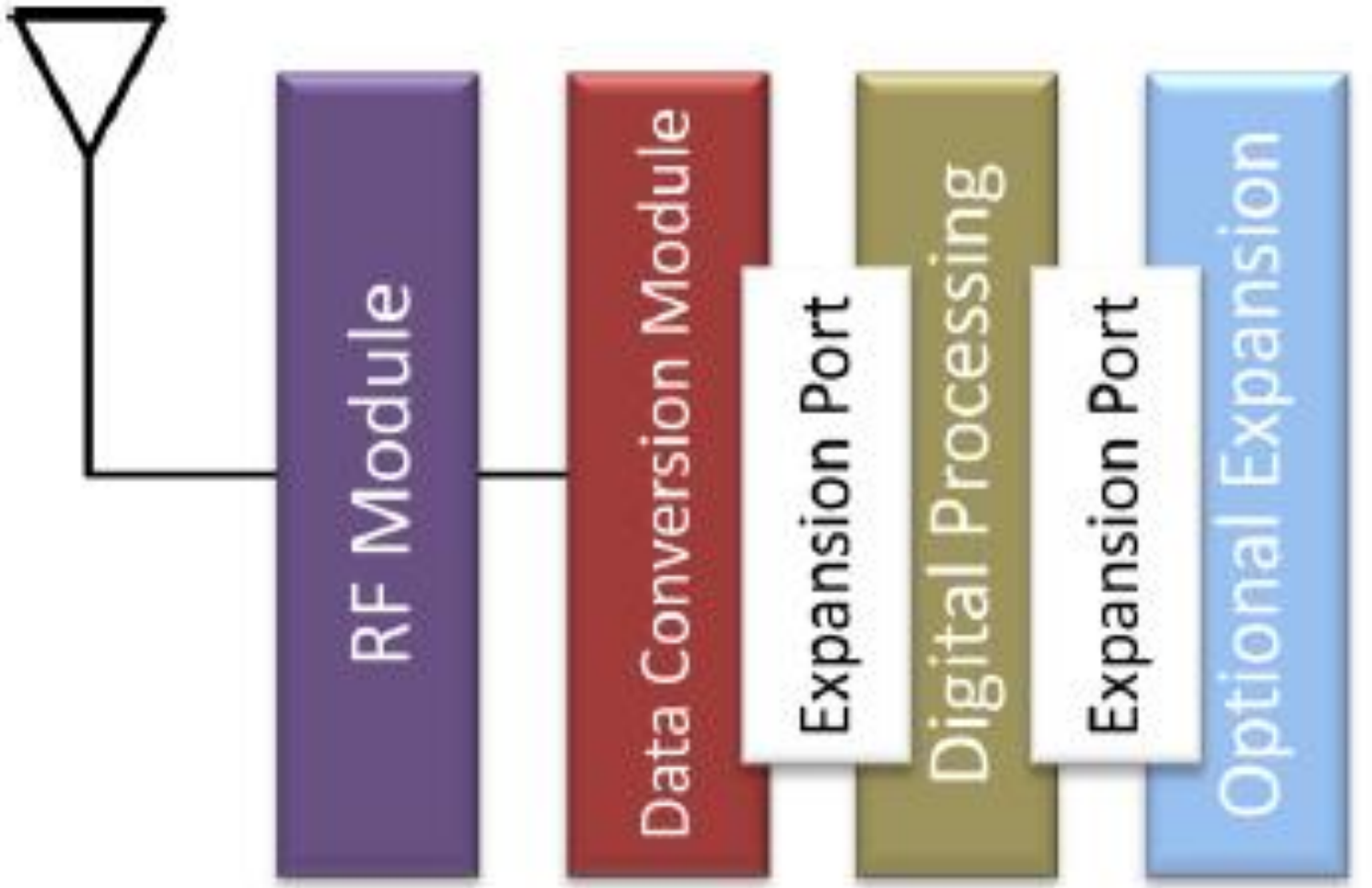



**FIGURE 3.** The software radio.

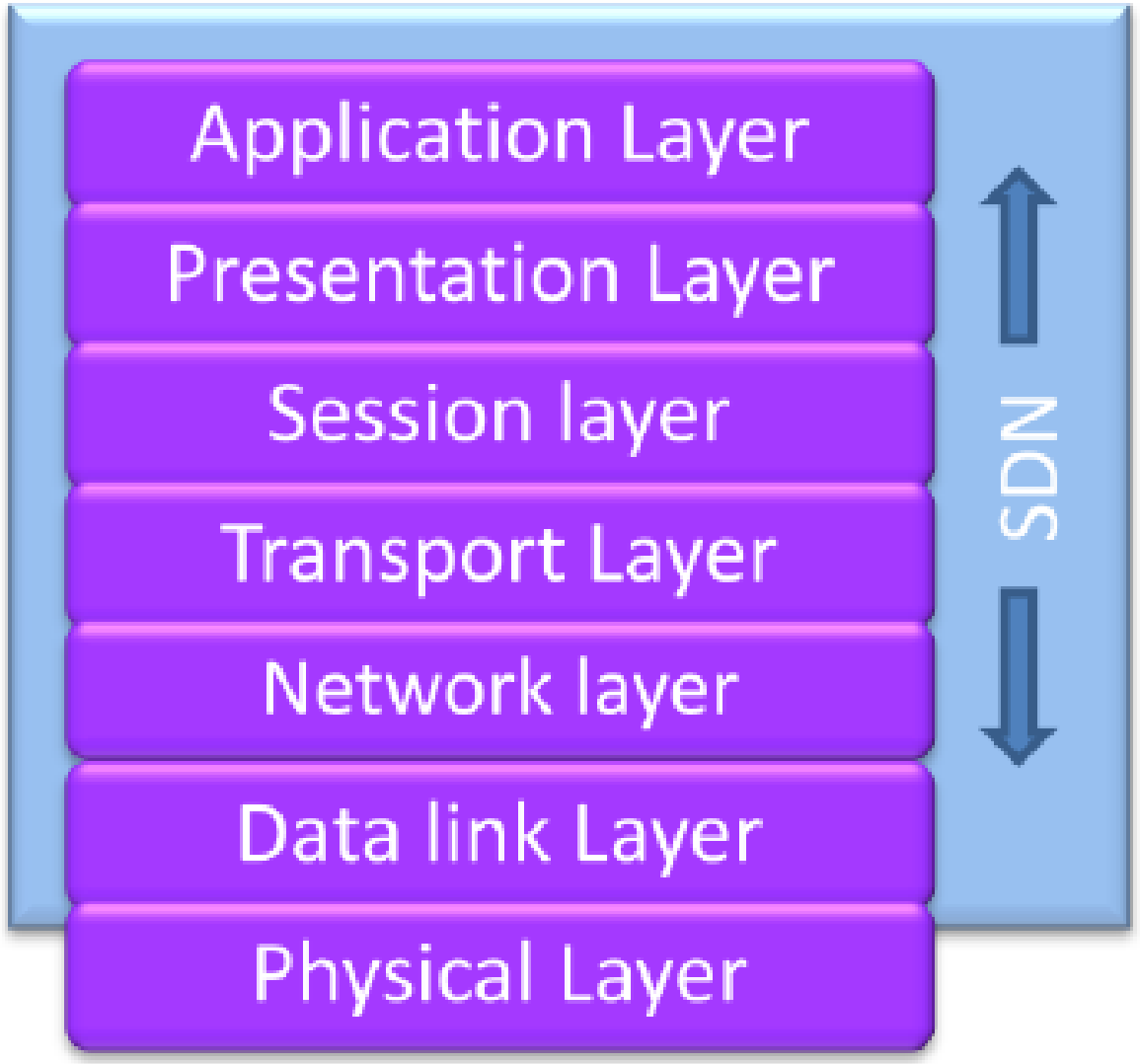



**FIGURE 4. SDN supports MAC layer to the application layer.**

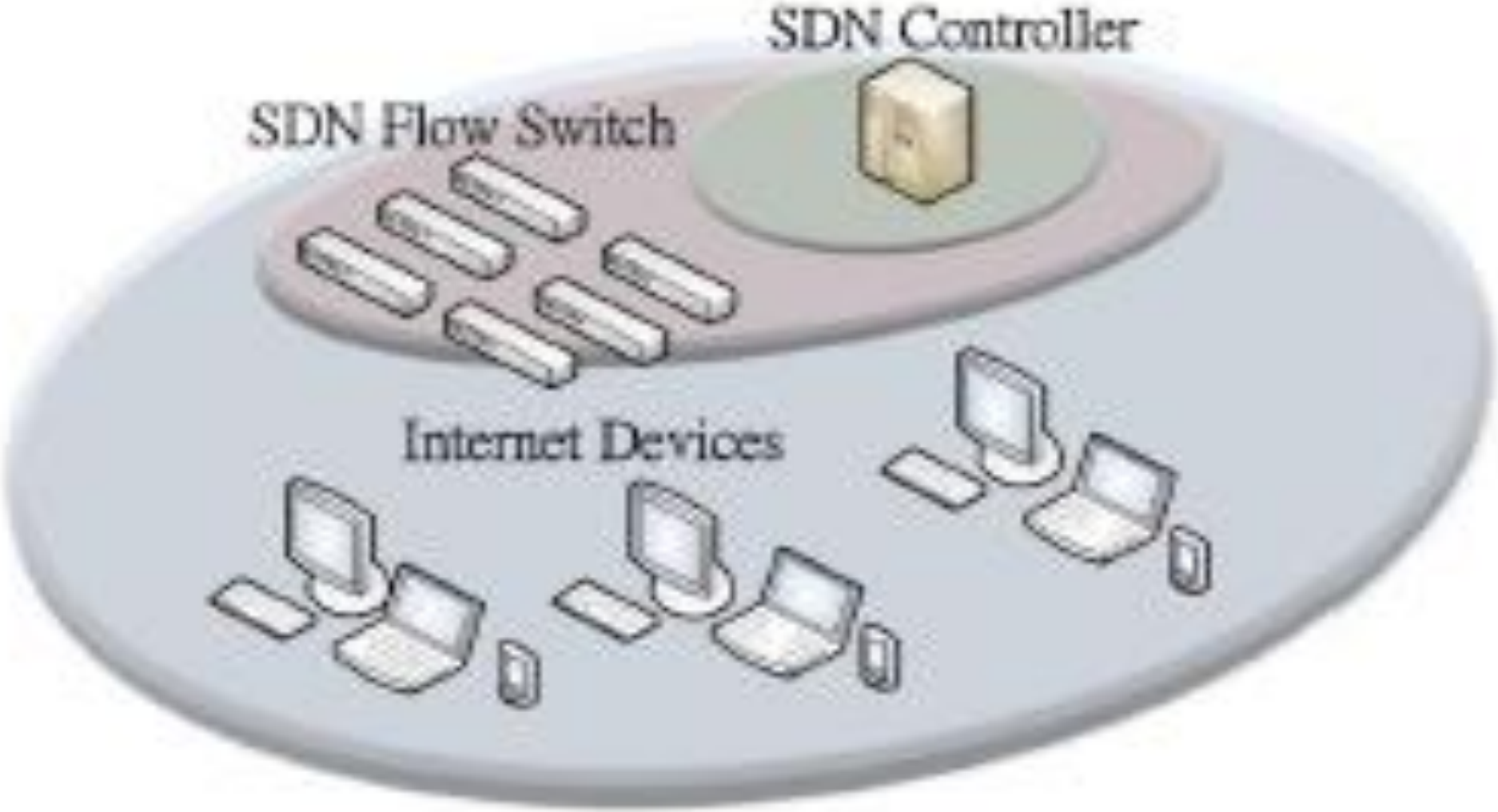



FIGURE 5. SDN architecture.

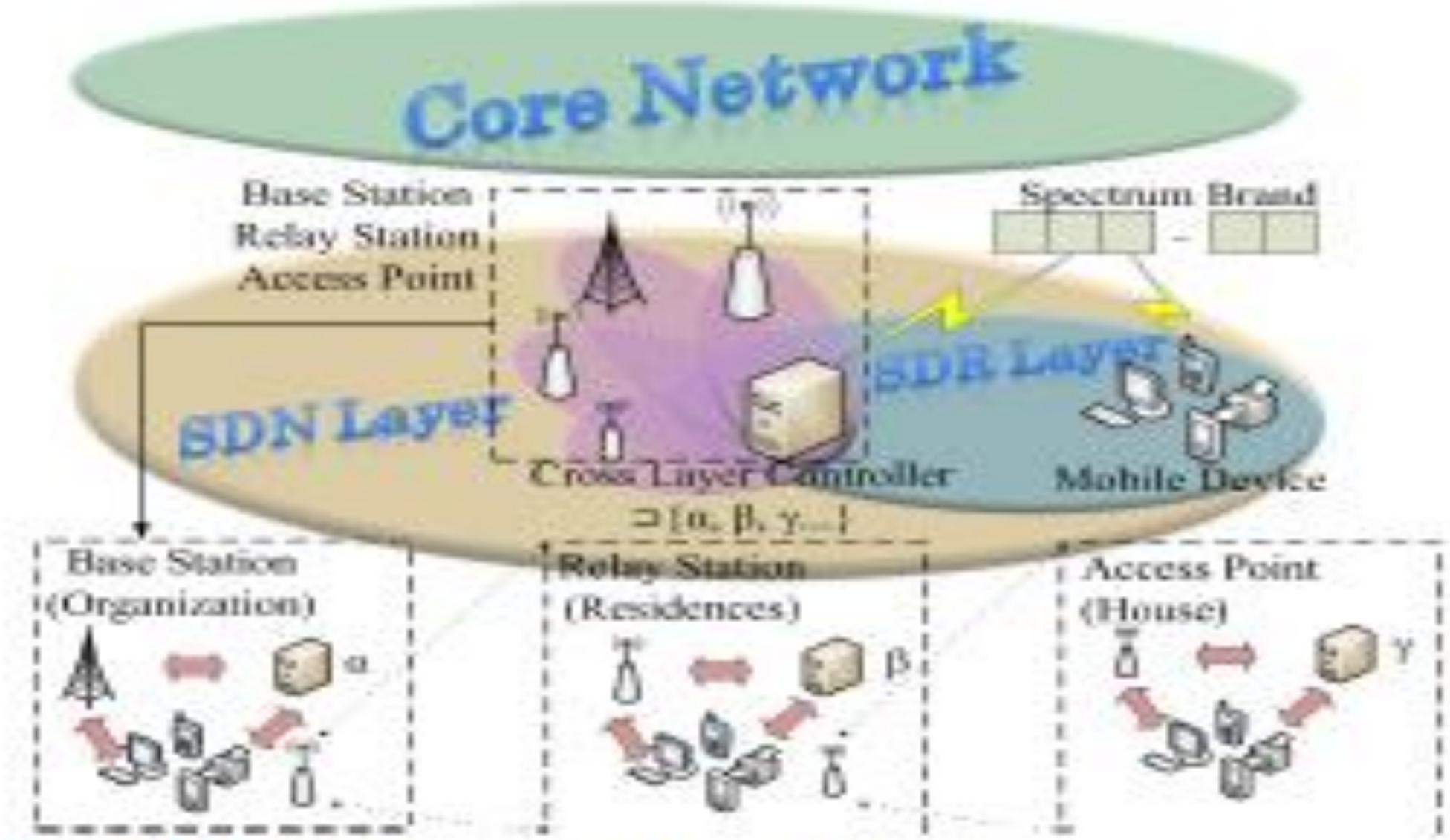
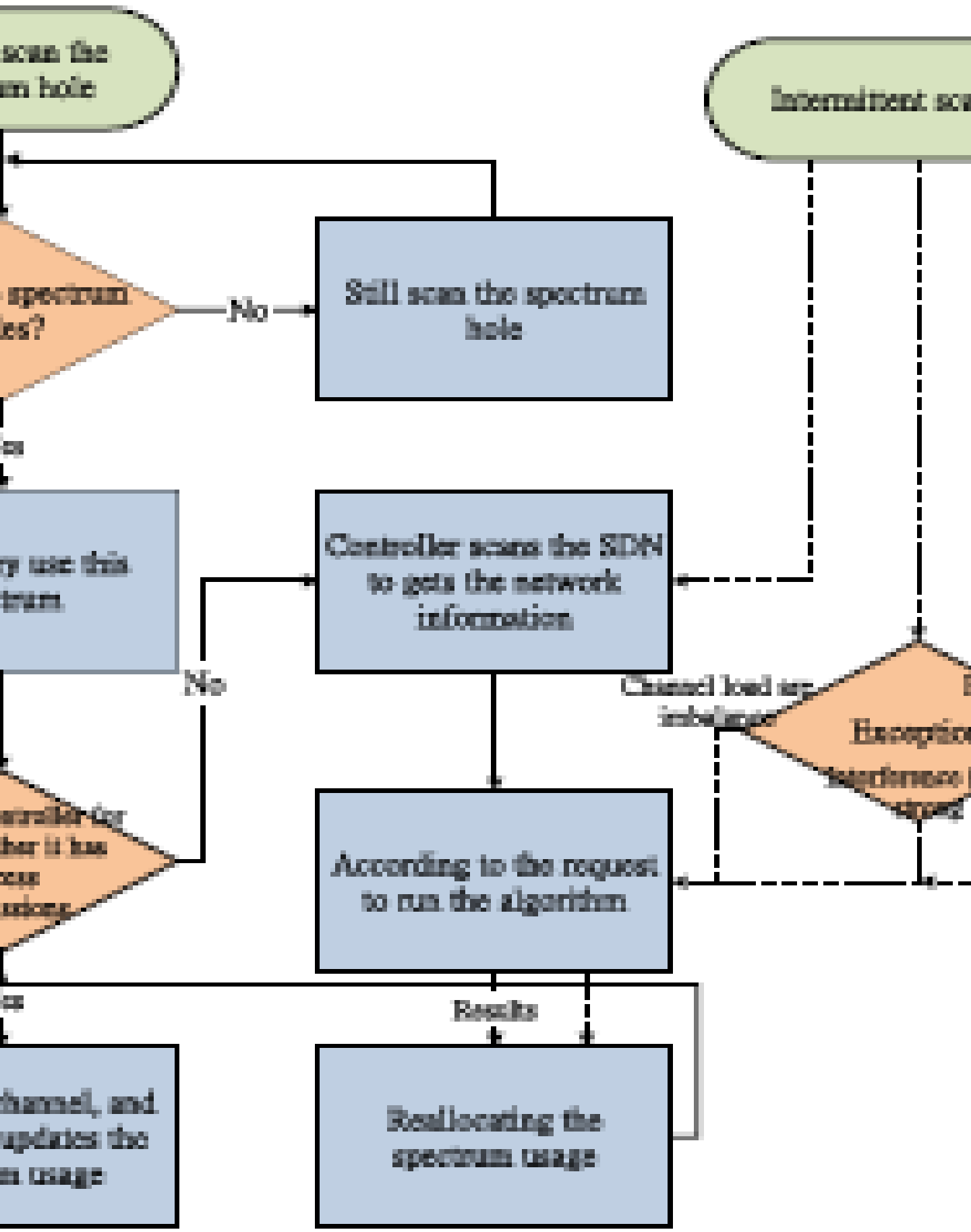



**FIGURE 6. Hybrid architecture of SDN and SDR.**




Detailed process of cross layer controller.

**TABLE 1. Simulation parameters.**

| *Parameters* | *Values* |
|---|---|
| Number of evaluated spectrums | 4 |
| Download frequency | 2140(MHz) |
| UpLink frequency | 1950(MHz) |
| Bandwidth | 60(MHz) |
| Number of evaluated devices | 10~100 |
| Interference parameter | 1~10 |

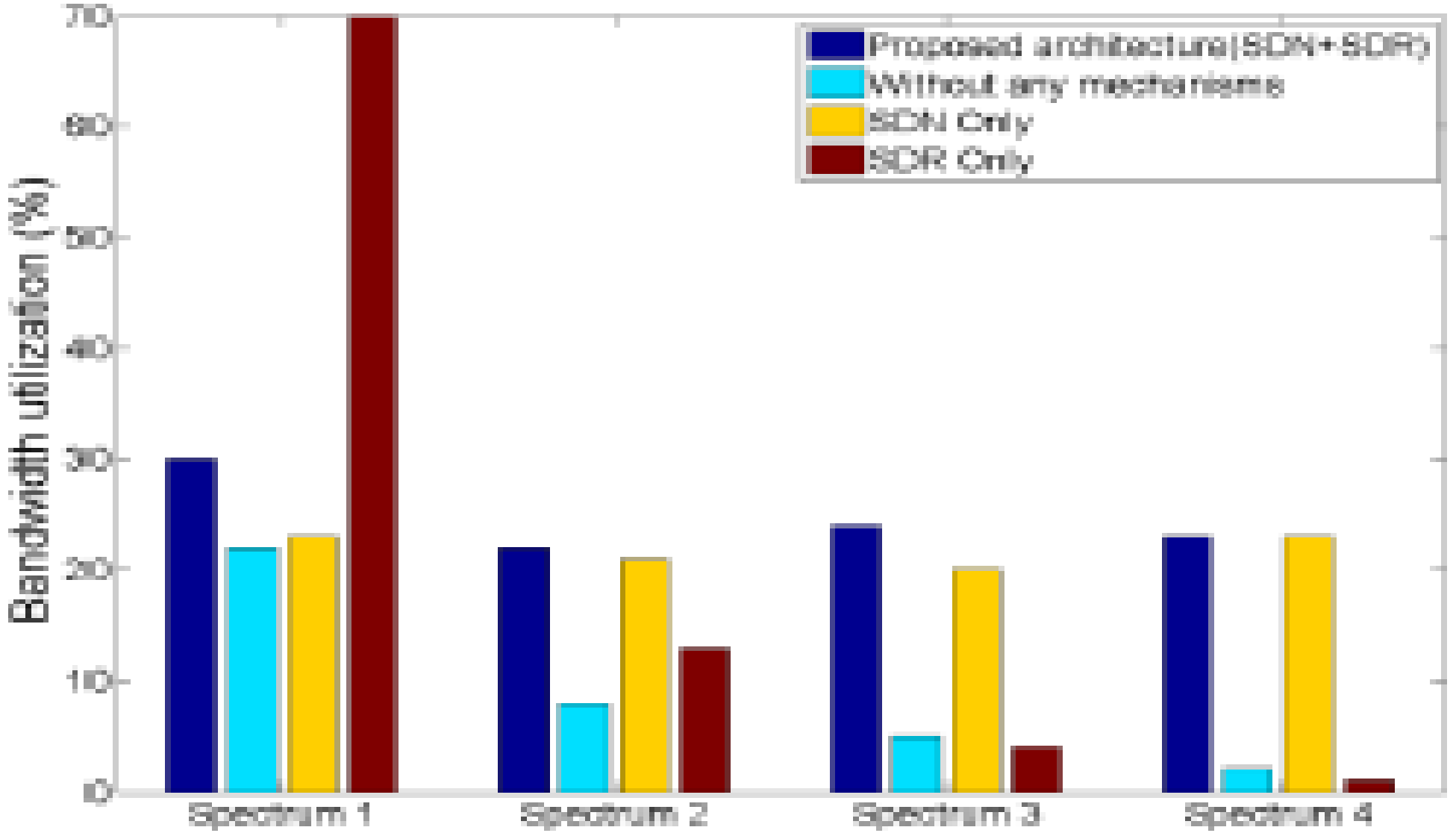



**FIGURE 8. Relationship between spectrum and bandwidth utilization rate.**

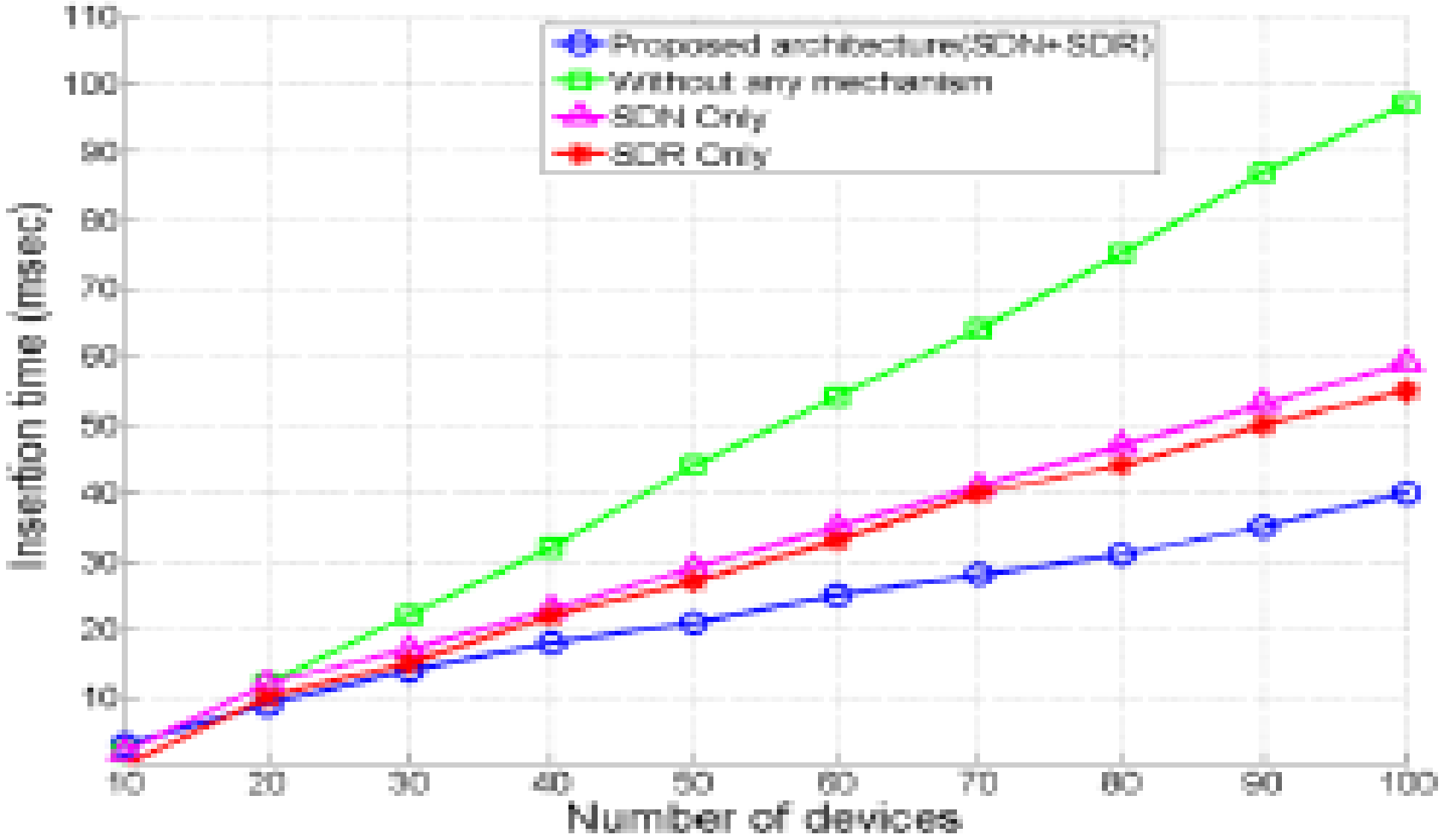



**FIGURE 9. Relationship between spectrum and bandwidth utilization rate.**

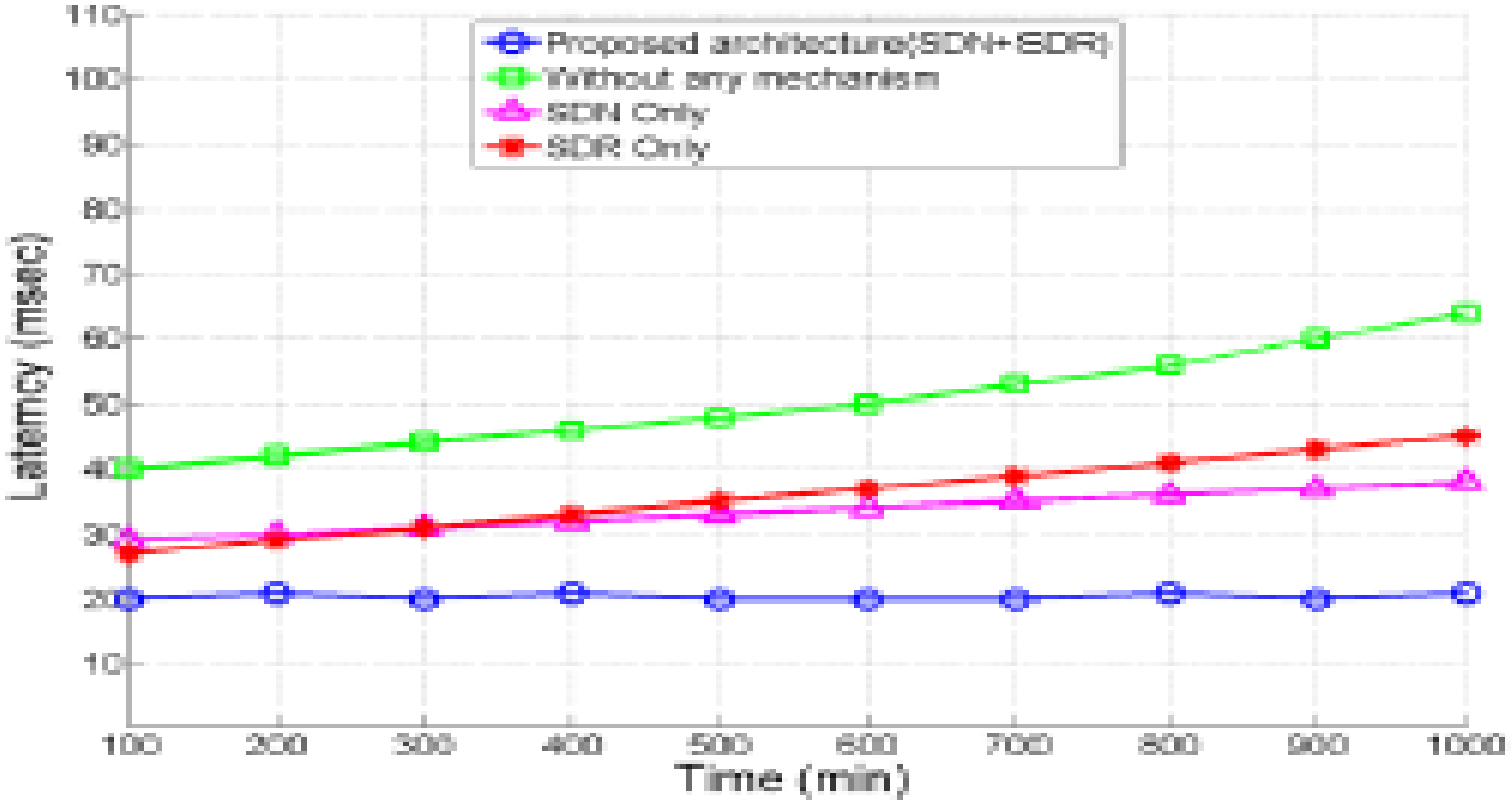



**FIGURE 10. Relationship between spectrum and bandwidth utilization rate.**

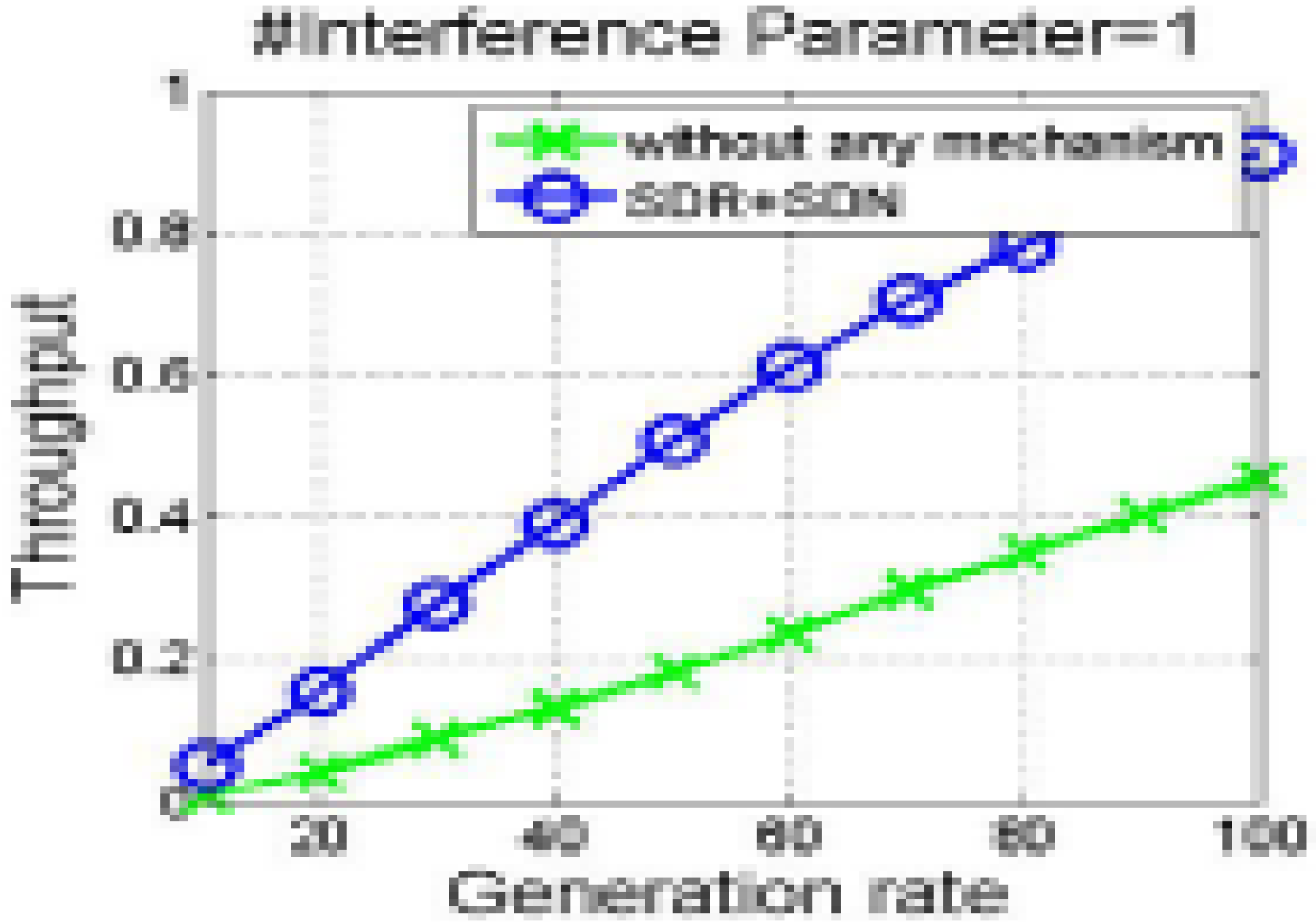



Figure 11. Relationship between spectrum and bandwidth utilisation rate

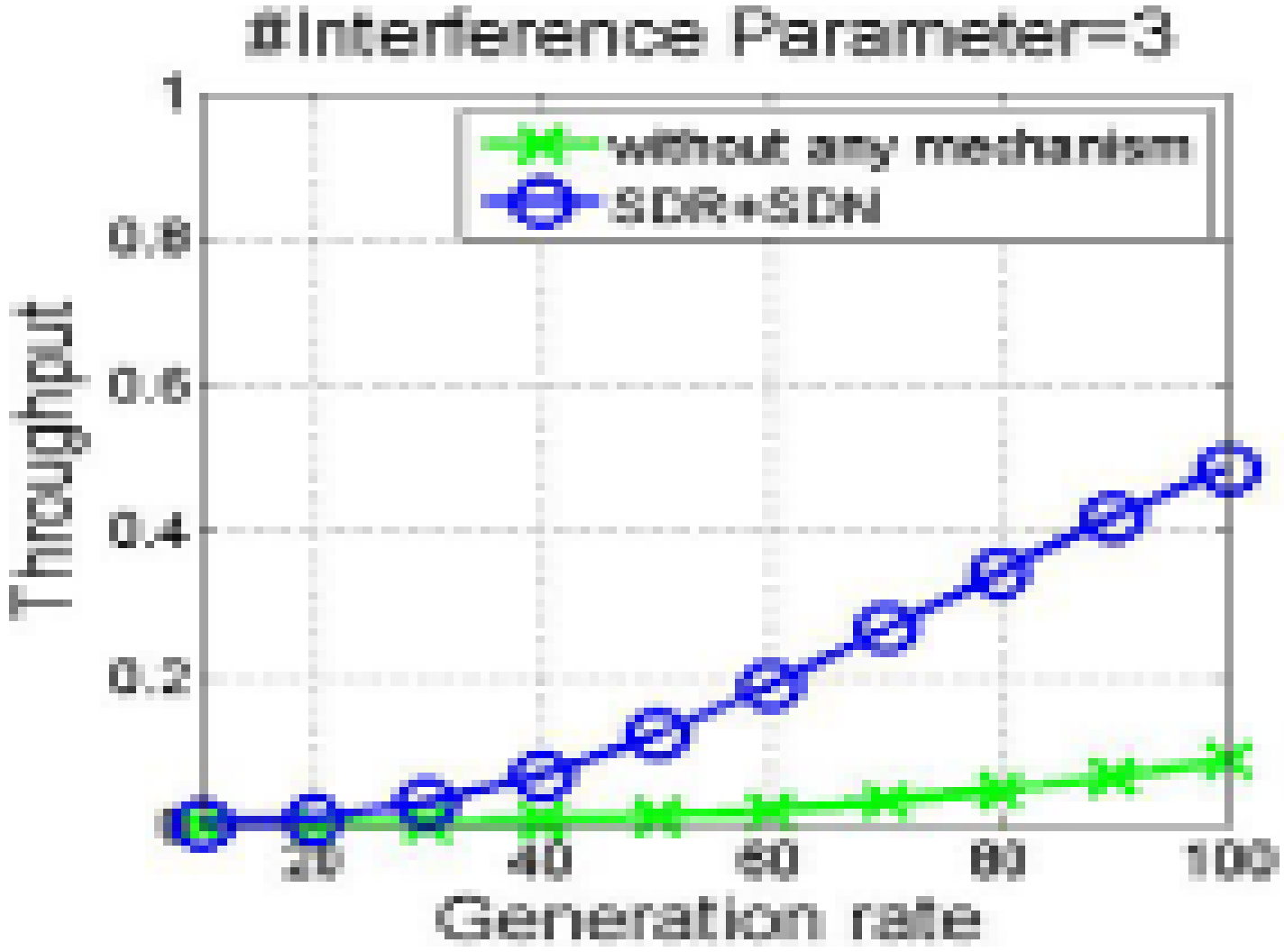



Figure 11. Relationship between spectrum and bandwidth utilisation rate

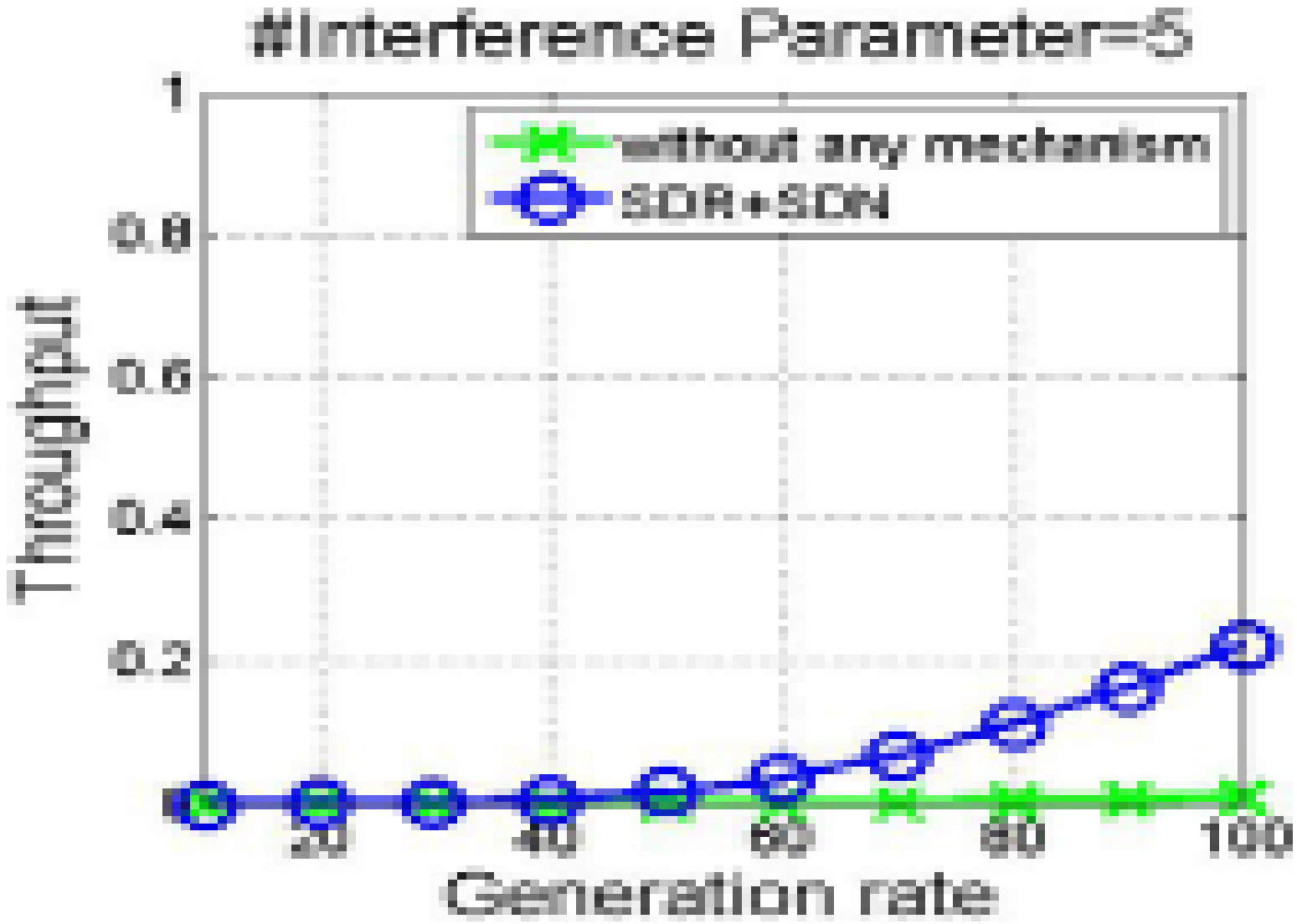



Figure 11. Relationship between spectrum and bandwidth utilisation rate

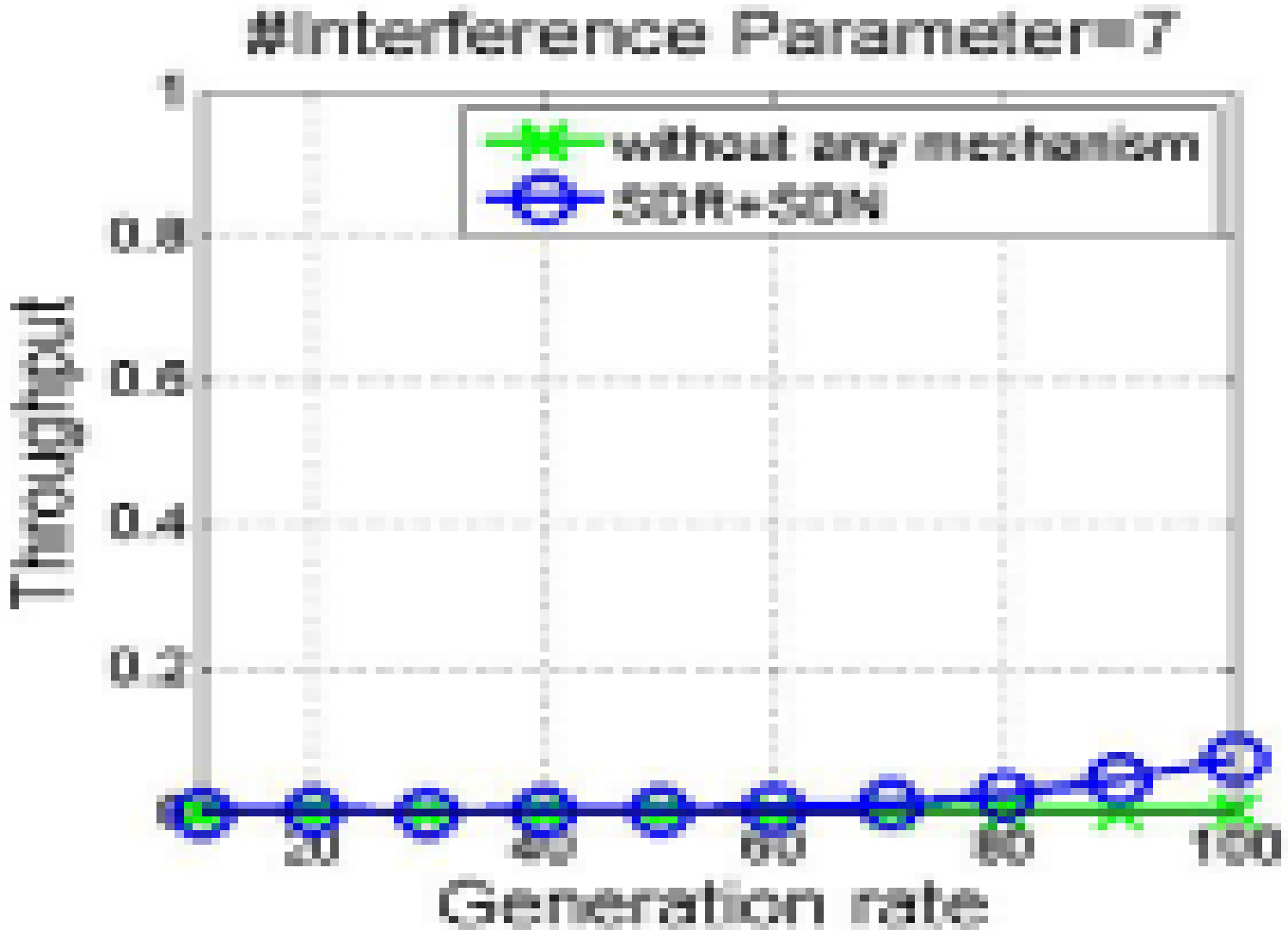



Figure 11. Relationship between spectrum and bandwidth utilisation rate

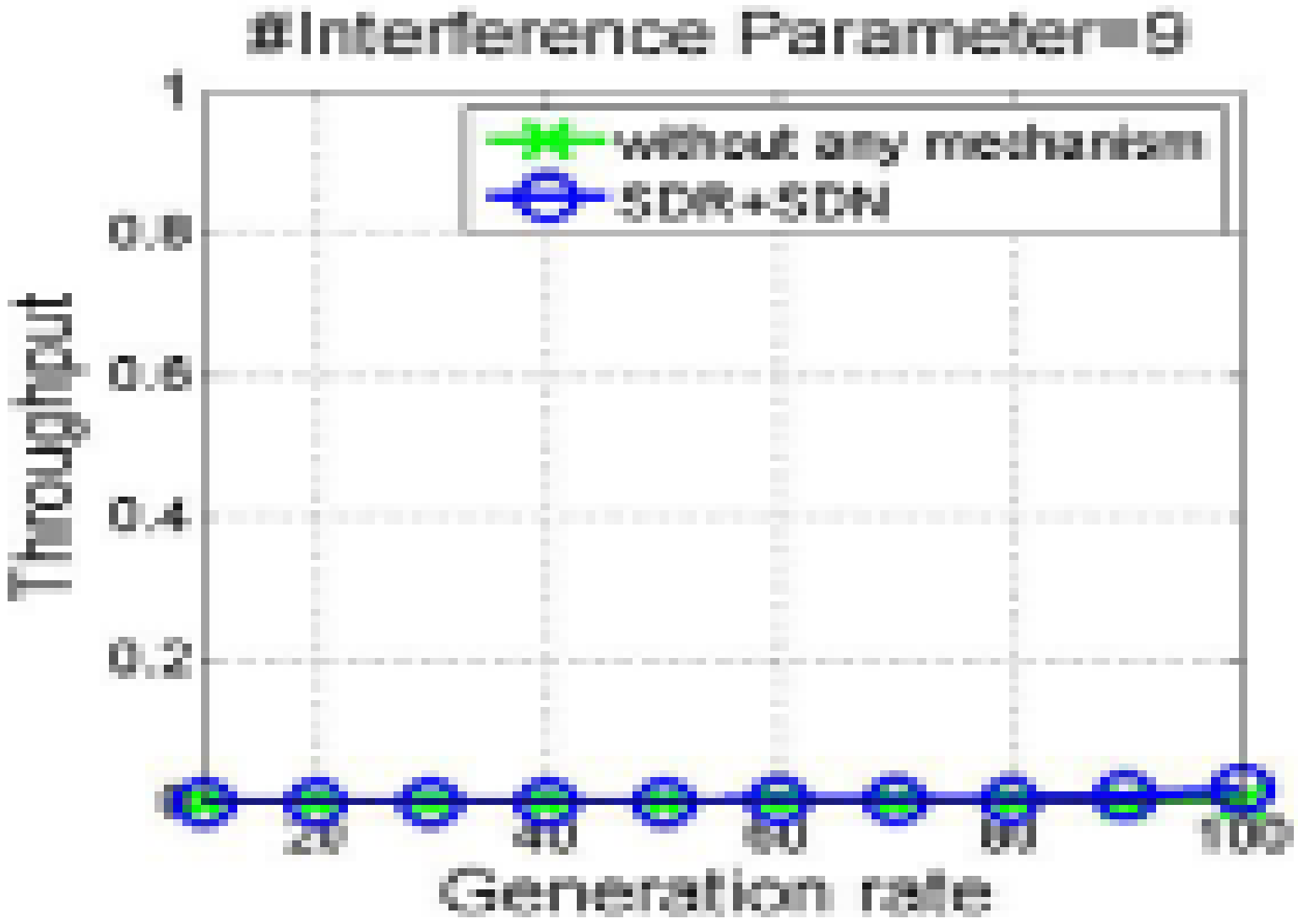



Figure 11. Relationship between spectrum and bandwidth utilisation rate

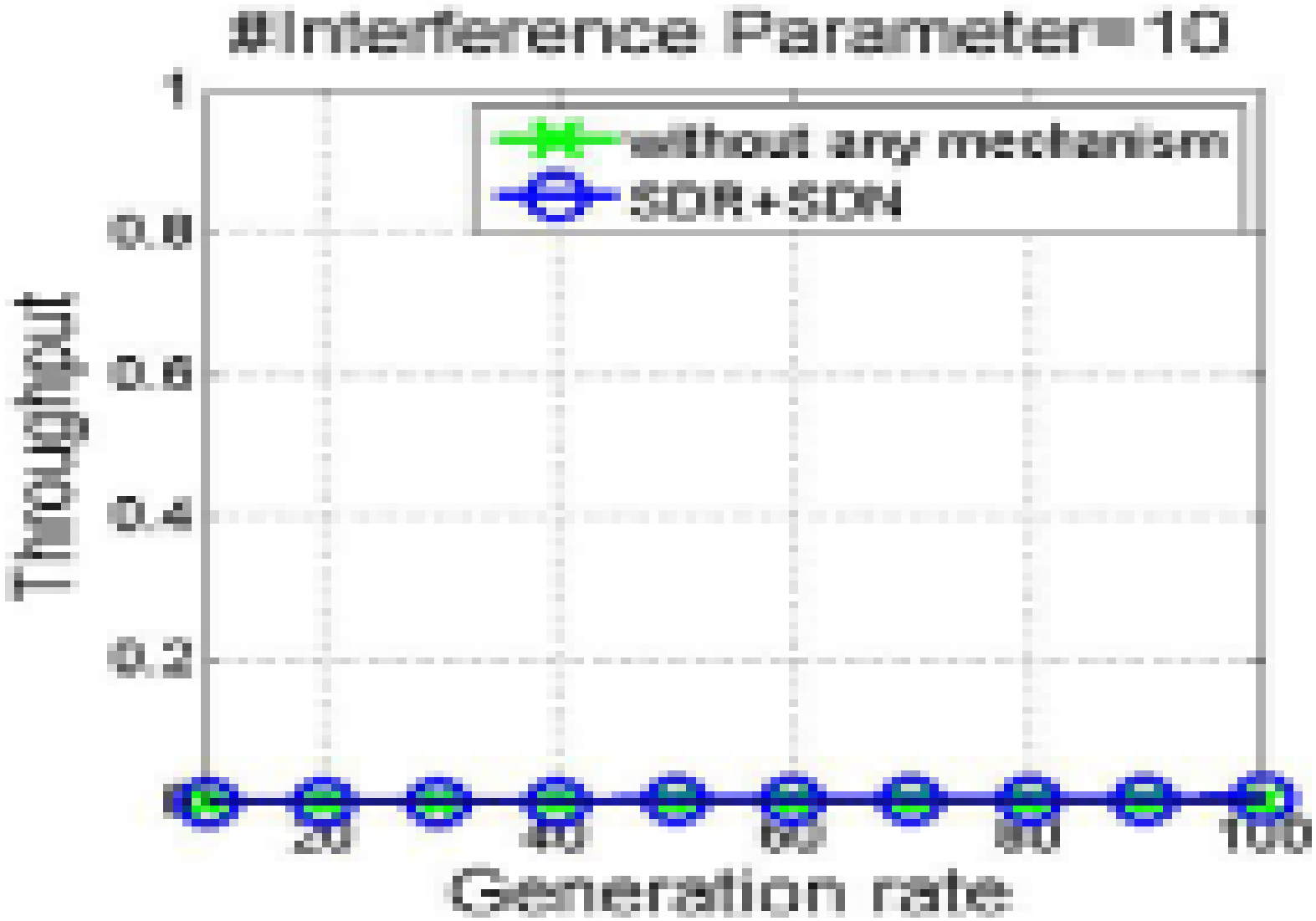
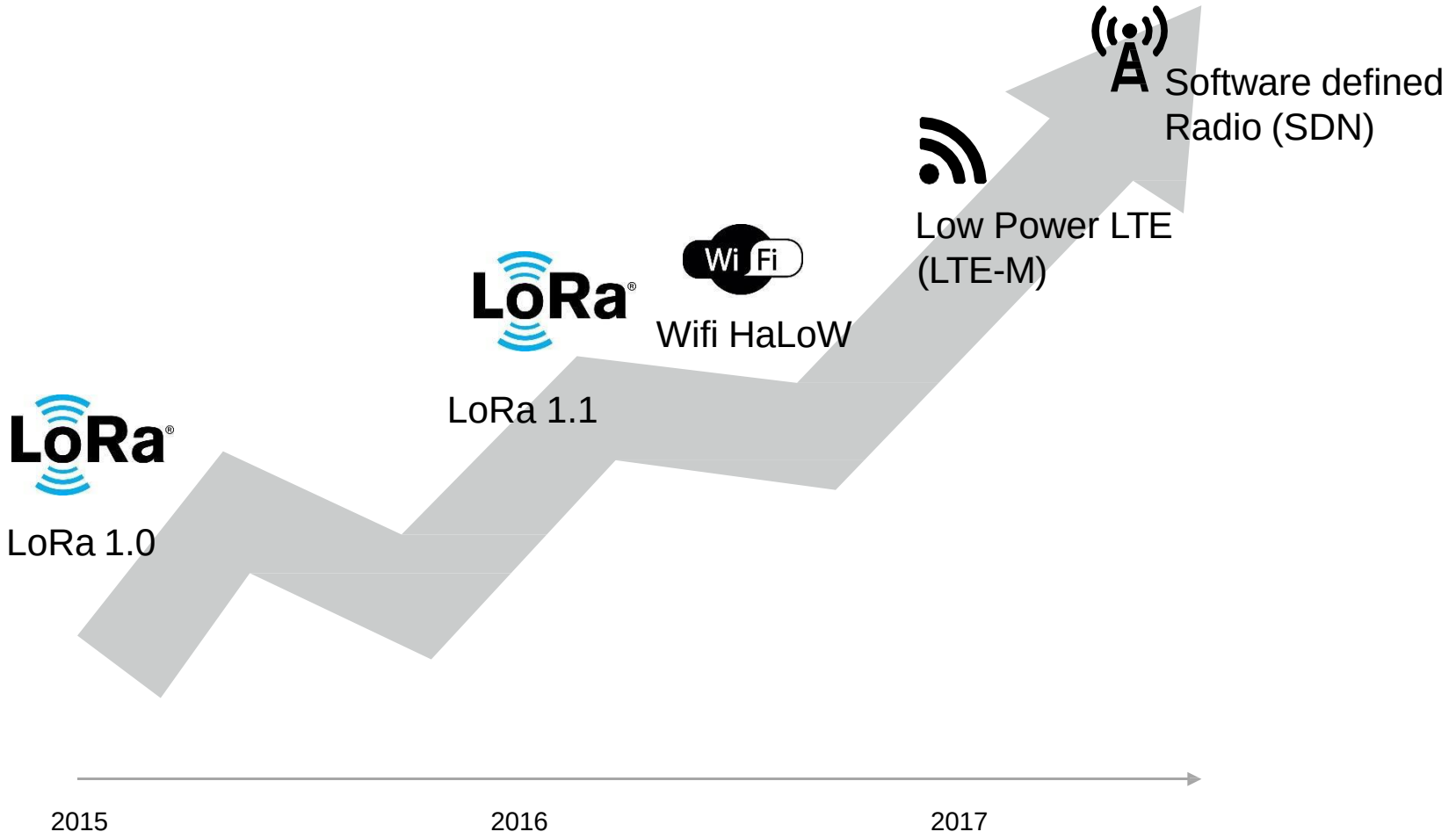



Figure 11. Relationship between spectrum and bandwidth utilisation rate

# Wireless IoT technologies – future outlook



# Internet of Things: Making the most of the Second digital Revolution - UK Government

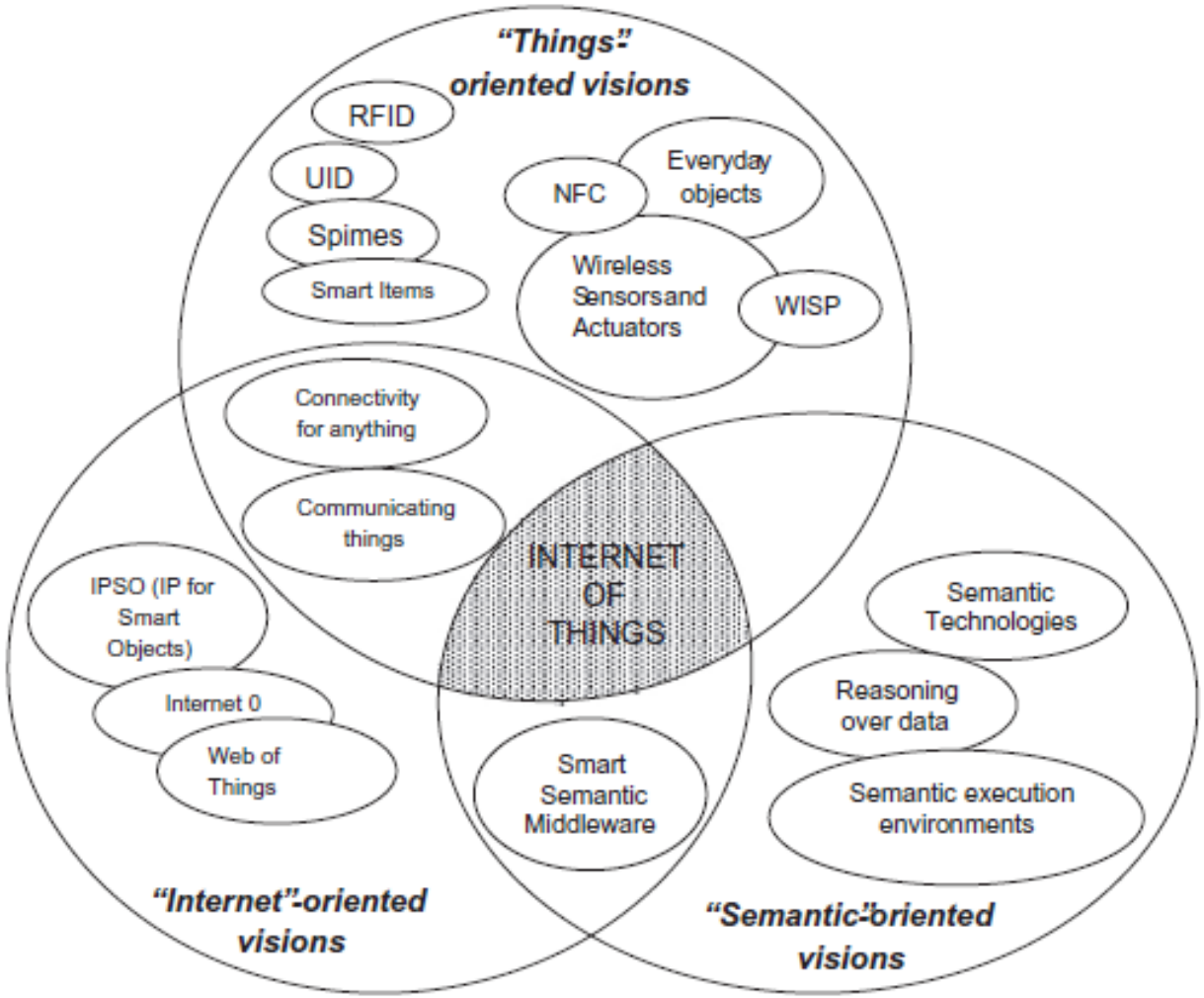
# Planning for support of IoT – By 2020, 25 to 50 billions of devices will connect to internet

"As more customers understand the IoT and its ready resources, they'll want to exploit them."

— Survey Respondent

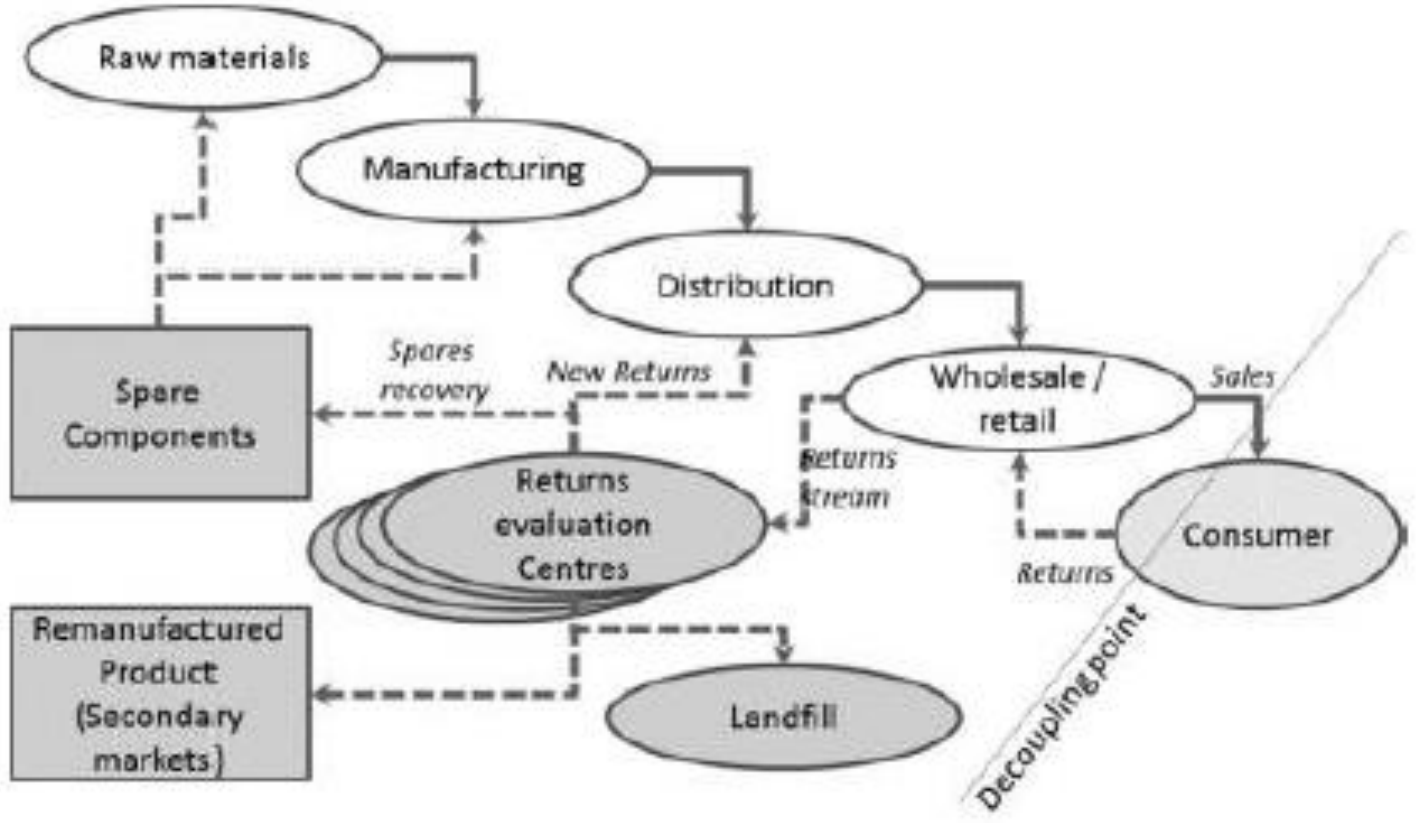
# Internet of Things Ecosystem

# Internet of things paradigm as a result of the convergence of different visions



# Operationalising IoT for reverse supply chain

**Figure 1** Generic integrated forward and reverse supply chain




**Source:** Adapted from Blackburn *et al.* (2004)

# SOA based middleware architecture

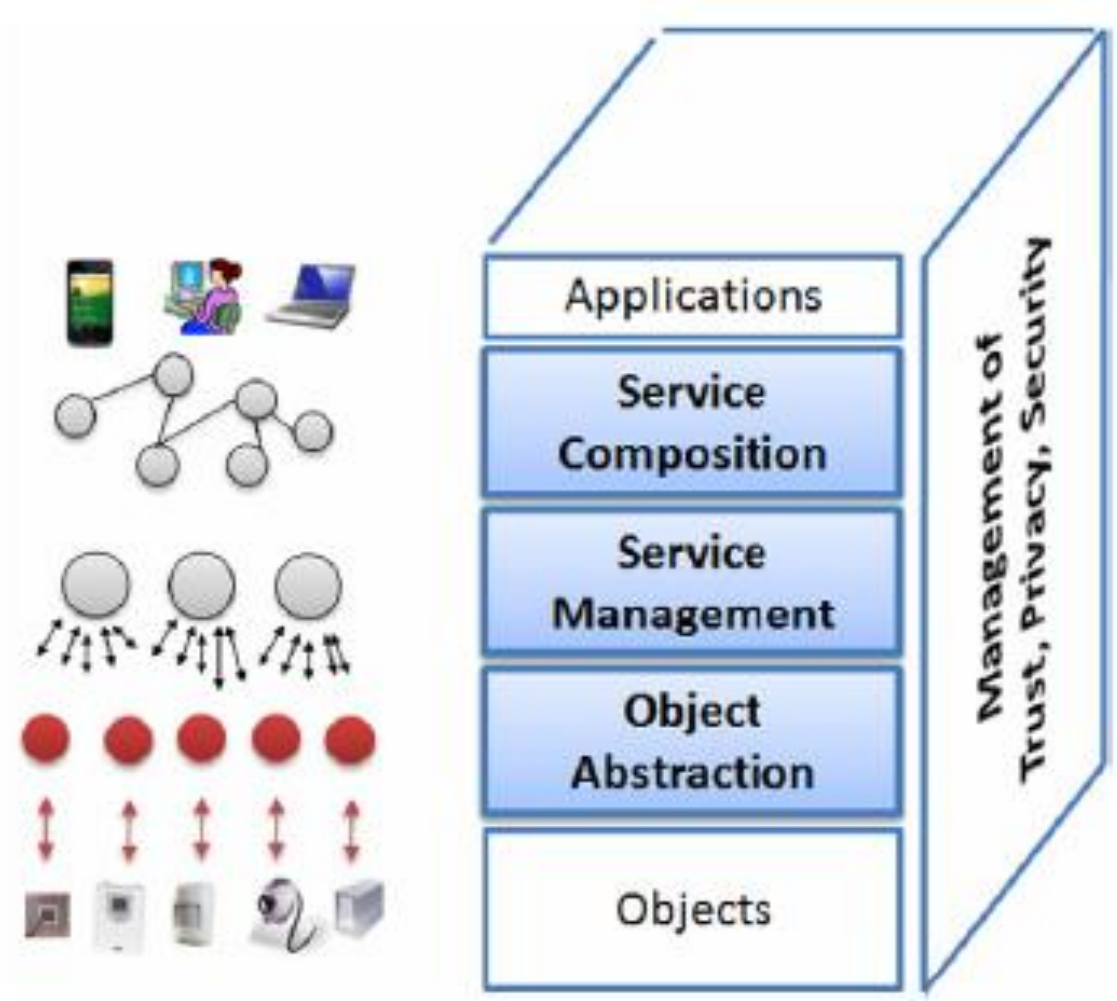


**Table 1**
Comparison between RFID systems, wireless sensor networks, and RFID sensor networks.

| | Processing | Sensing | Communication | Range (m) | Power | Lifetime | Size | Standard |
|---|---|---|---|---|---|---|---|---|
| RFID | No | No | Asymmetric | 10 | Harvested | Indefinite | Very small | ISO18000 |
| WSN | Yes | Yes | Peer-to-peer | 100 | Battery | <3 years | Small | IEEE 802.15.4 |
| RSN | Yes | Yes | Asymmetric | 3 | Harvested | Indefinite | Small | None |

# IOT Applications Domains and relevant scenarios

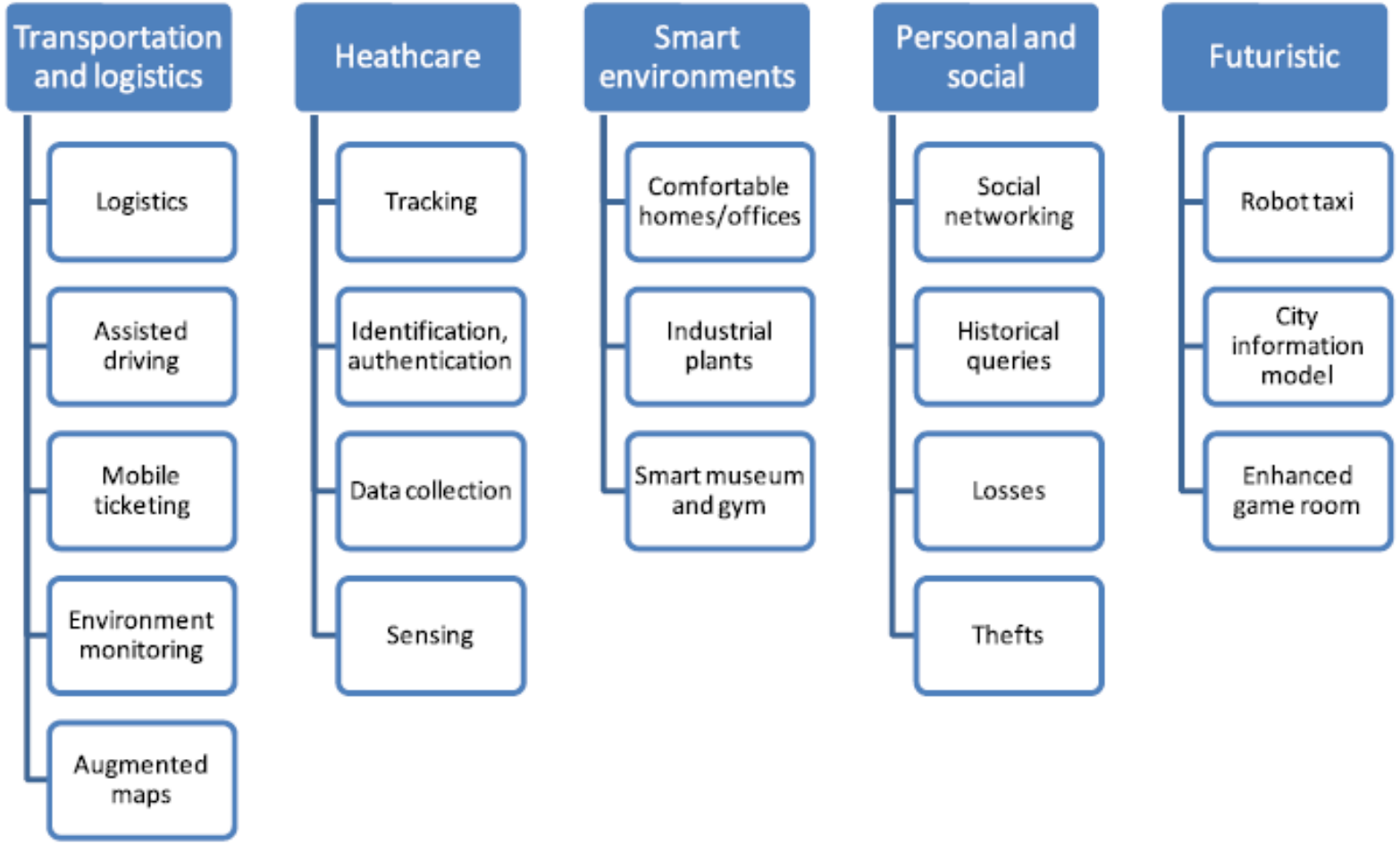


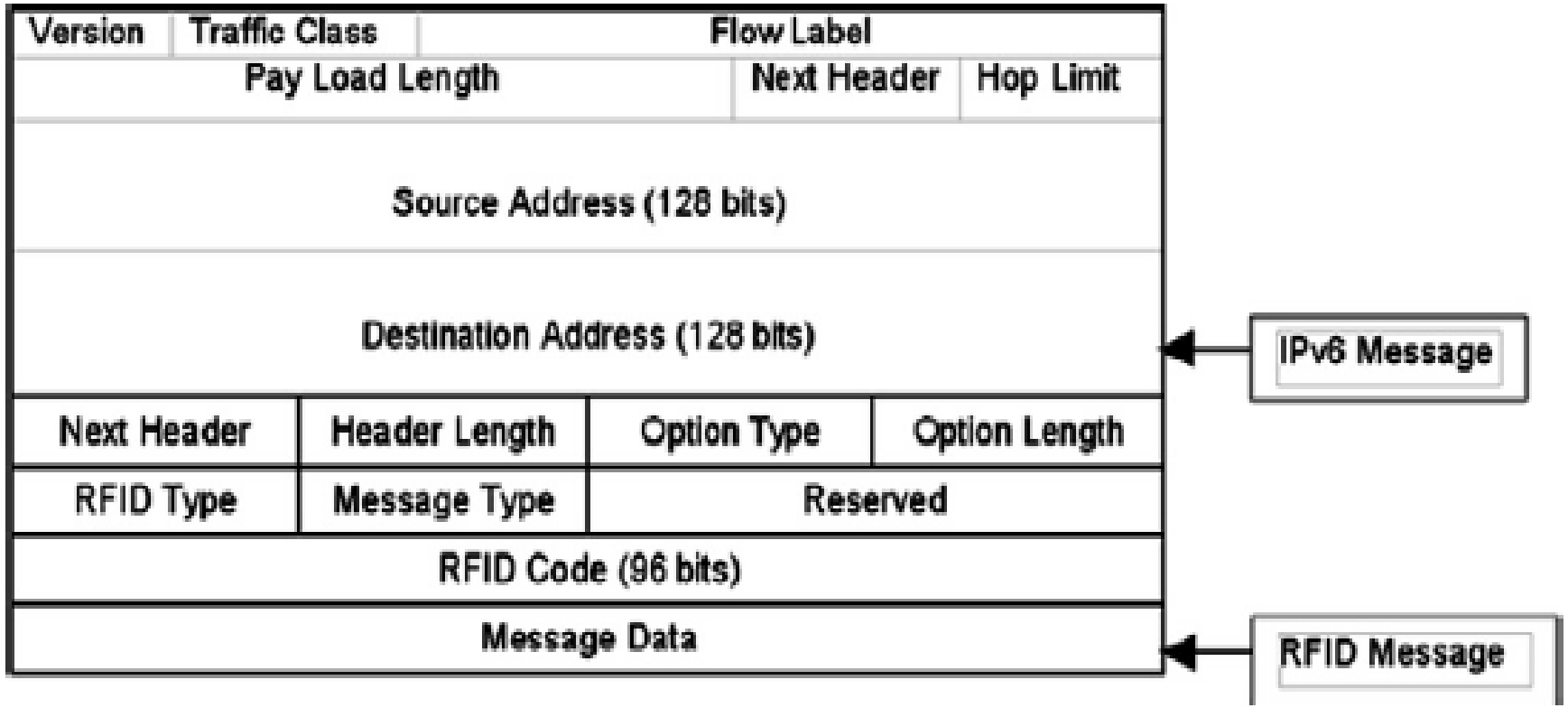
**Table 2**
Open research issues.

| Open issue | Brief description of the cause | Details in |
|---|---|---|
| Standards | There are several standardization efforts but they are not integrated in a comprehensive framework | Section 5.1 |
| Mobility support | There are several proposals for object addressing but none for mobility support in the IoT scenario, where scalability and adaptability to heterogeneous technologies represent crucial problems | Section 5.2 |
| Naming | Object Name Servers (ONS) are needed to map a reference to a description of a specific object and the related identifier, and *vice versa* | Section 5.2 |
| Transport protocol | Existing transport protocols fail in the IoT scenarios since their connection setup and congestion control mechanisms may be useless; furthermore, they require excessive buffering to be implemented in *objects* | Section 5.2 |
| Traffic characterization and QoS support | The IoT will generate data traffic with patterns that are expected to be significantly different from those observed in the current Internet. Accordingly, it will also be necessary to define new QoS requirements and support schemes | Section 5.2 |
| Authentication | Authentication is difficult in the IoT as it requires appropriate authentication infrastructures that will not be available in IoT scenarios. Furthermore, things have scarce resources when compared to current communication and computing devices. Also man-in-the-middle attack is a serious problem | Section 5.3 |
| Data integrity | This is usually ensured by protecting data with passwords. However, the password lengths supported by IoT technologies are in most cases too short to provide strong levels of protection | Section 5.3 |
| Privacy | A lot of private information about a person can be collected without the person being aware. Control on the diffusion of all such information is impossible with current techniques | Section 5.3 |
| Digital forgetting | All the information collected about a person by the IoT may be retained indefinitely as the cost of storage decreases. Also data mining techniques can be used to easily retrieve any information even after several years | Section 5.3 |

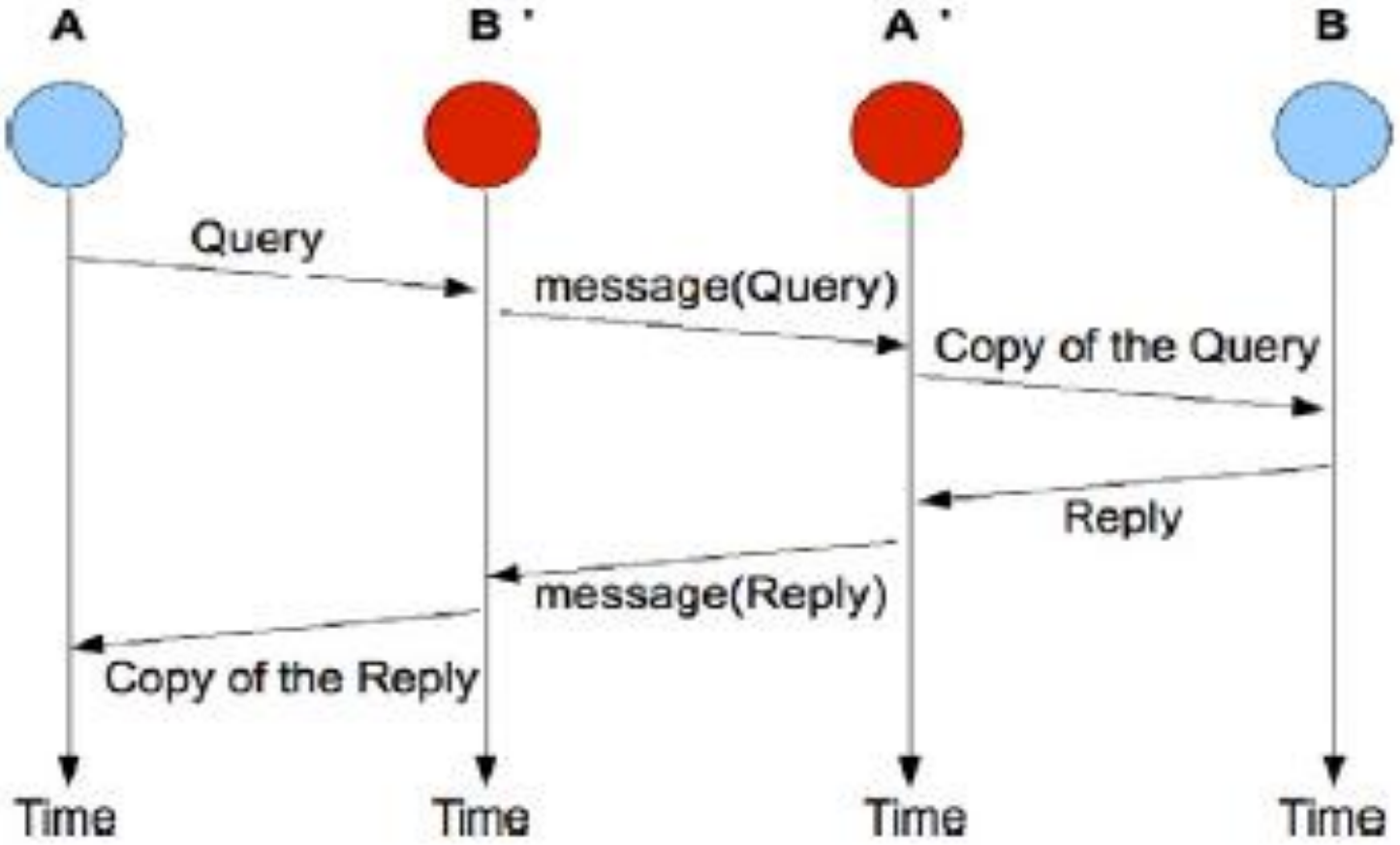
**Table 3**
Characteristics of the most relevant standardization activities.

| Standard | Objective | Status | Comm. range (m) | Data rate (kbps) | Unitary cost ($) |
|---|---|---|---|---|---|
| *Standardization activities discussed in this section* | | | | | |
| EPCglobal | Integration of RFID technology into the electronic product code (EPC) framework, which allows for sharing of information related to products | Advanced | ~1 | ~$10^2$ | ~0.01 |
| GRIFS | European Coordinated Action aimed at defining RFID standards supporting the transition from localized RFID applications to the *Internet of Things* | Ongoing | ~1 | ~$10^2$ | ~0.01 |
| M2M | Definition of cost-effective solutions for machine-to-machine (M2M) communications, which should allow the related market to take off | Ongoing | N.S. | N.S. | N.S. |
| 6LoWPAN | Integration of low-power IEEE 802.15.4 devices into IPv6 networks | Ongoing | 10–100 | ~$10^2$ | ~1 |
| ROLL | Definition of routing protocols for heterogeneous low-power and lossy networks | Ongoing | N.S. | N.S. | N.S. |
| *Other relevant standardization activities* | | | | | |
| NFC | Definition of a set of protocols for low range and bidirectional communications | Advanced | ~$10^{-2}$ | Up to 424 | ~0.1 |
| Wireless Hart | Definition of protocols for self-organizing, self-healing and mesh architectures over IEEE 802.15.4 devices | Advanced | 10–100 | ~$10^2$ | ~1 |
| ZigBee | Enabling reliable, cost-effective, low-power, wirelessly networked, monitoring and control products | Advanced | 10–100 | ~$10^2$ | ~1 |

# Encapsulation of RFID message into an IPv6 packet



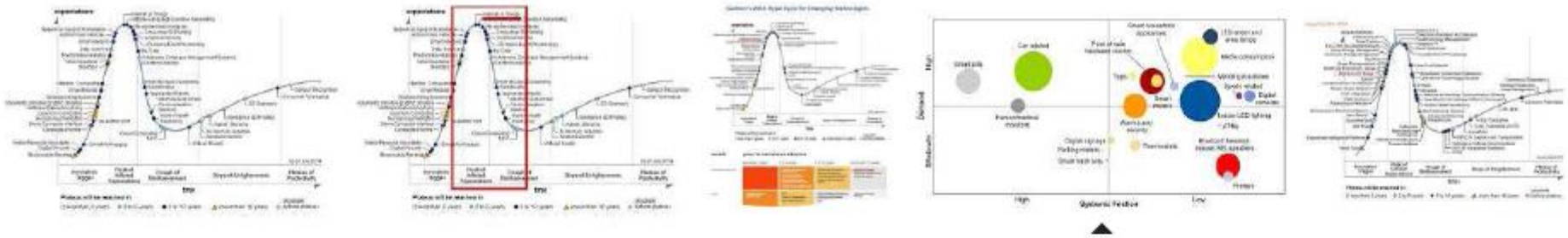
# Man in the middle of attack (or proxy attack)

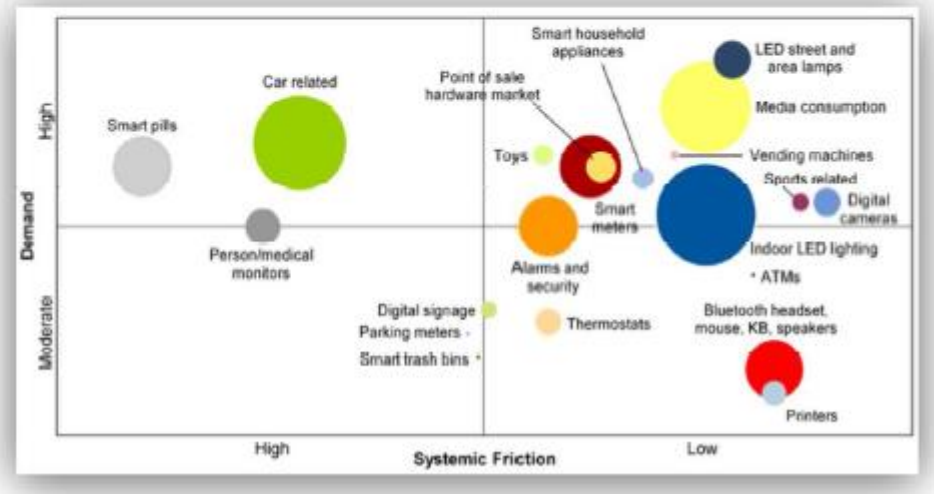


# Security and privacy of IoT –Authentication & data integrity

Extremely vulnerable to attack due to

1. Mostly unattended components
2. Most of communication are wireless – eavesdropping simple
3. Use low energy component –hard to implement complex







Gartner (2014) study of IoT

# Intelligent Transport System: connected vehicles, cloud computing and Internet of Things

Antonio J., Ibanez G., Zeadally S. and Contreras-Castillo, J. Integration Challenges of Intelligent Transportation Systems with Connected Vehicles, Cloud Computing, and Internet of Things Technologies, IEEE wireless Communications, Dec 2015, pp. 122-128.

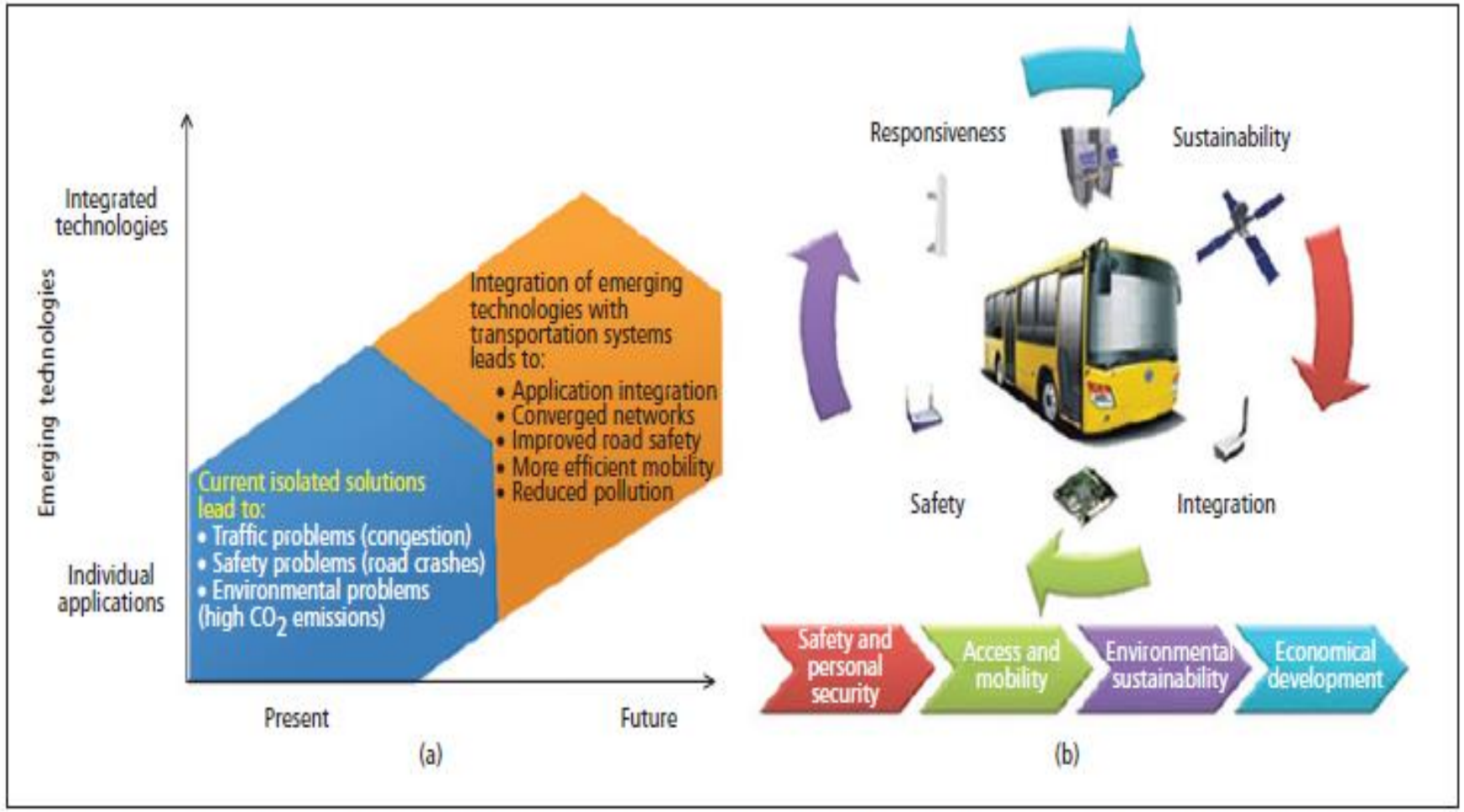



**Figure 1.** a) Future trends of intelligent transportation systems; b) impact of emerging technologies on ITS.

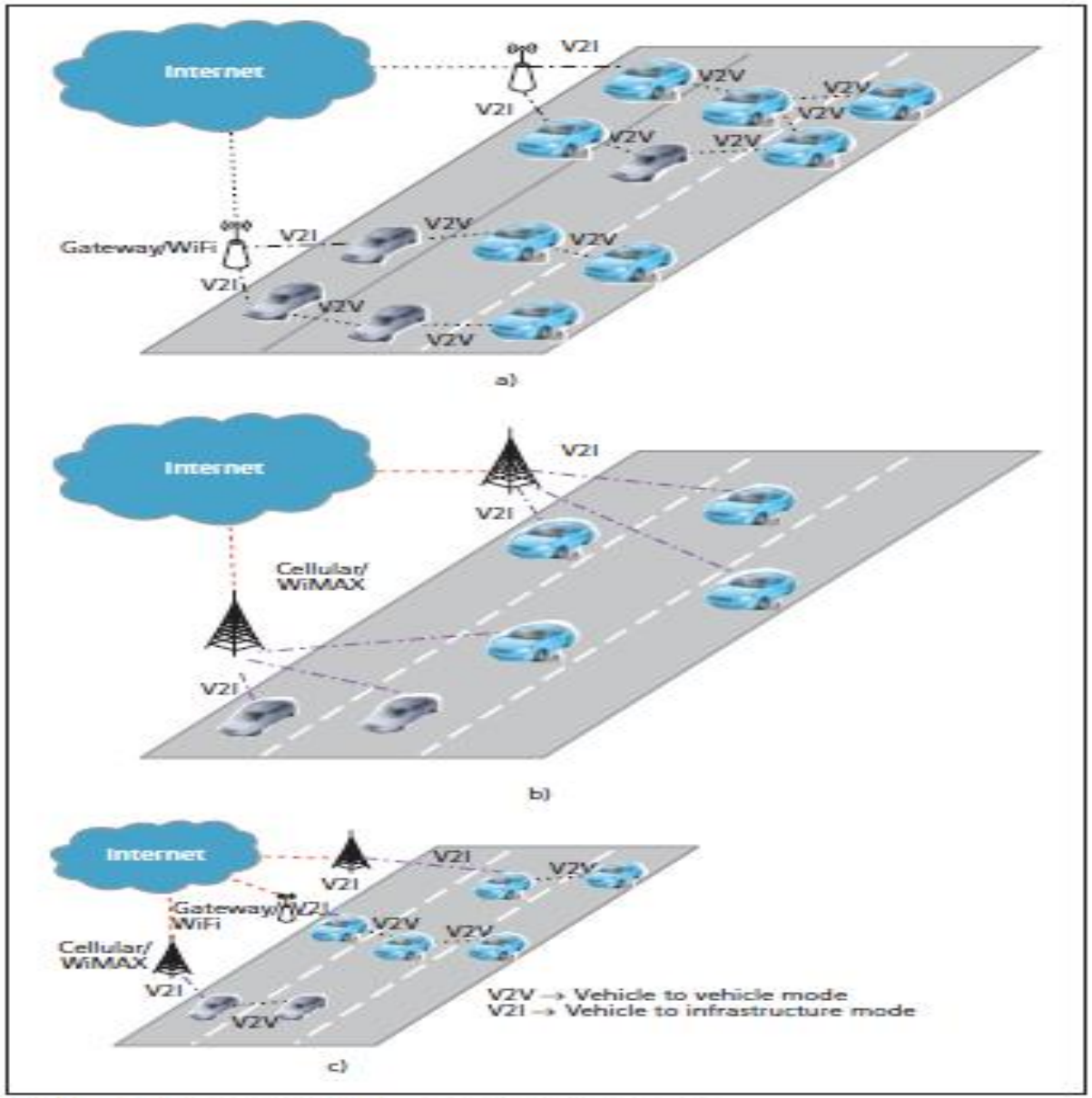



**Figure 2.** Wireless vehicular networking scenarios.

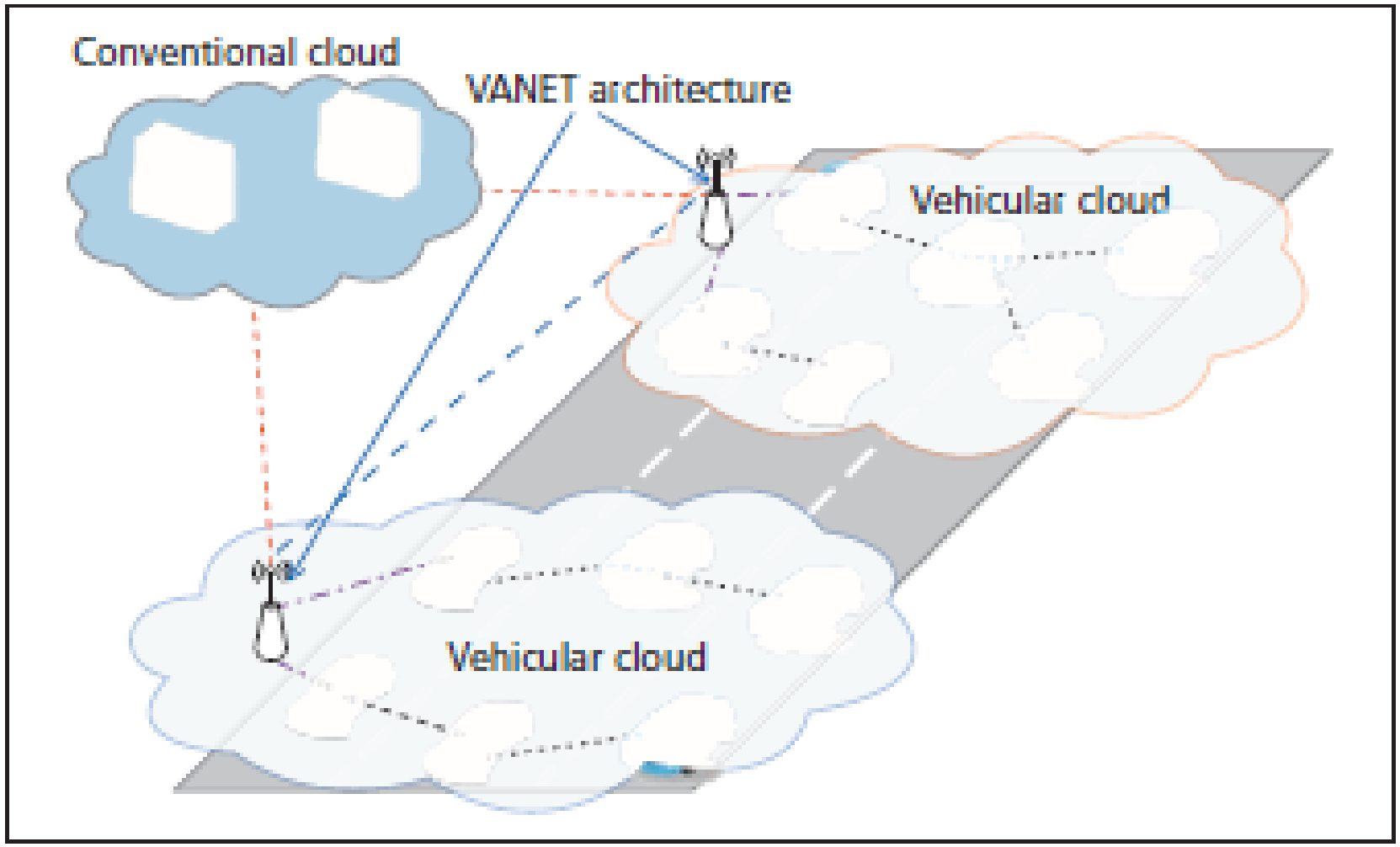



Figure 3. Vehicular Cloud architecture.

# Five Guidelines on Cloud Computing

1. Hybrid cloud computing is the definitive model.
2. Focus on “as-a-strategy”—software (SaaS), infrastructure (IaaS), and platform (PaaS).
3. Network and data security are key; security must be built into the architecture.
4. Bi-modal IT is dead; the world is increasingly agile.
5. It is better to fail forward, than to stagnate not trying.

# Deploying next generation cyber security

VMWare white paper (Feb 2018) - Rethinking security strategy to meet next-generation security challenges

Micro-segmentation is a new cybersecurity solution for SME. There are three steps in developing an effective micro-segmentation process.

Step 1 - Determine the network flow in entire enterprise

Step 2 - Identify patterns and relationships in the traffic

Step 3 - Create and apply the policy model (e.g. apply one micro-segmentation at a time.

# Tips and tricks for a successful micro-segmentation deployment

1. Utilize Application Rule Manager (e.g. VMware' ARM)
2. Maps out security group
3. Develop consistent naming conventions for security groups
4. Build a cross-functional team to support micro-segmentation development

# Architecture and design patterns

## Examples of architecture patterns

1. Authentication architecture
2. Authorisation frameworks
3. Cloud-based system architecture
4. Mobile application architectures
5. Microservices-based architecture
6. Containerization

# Key benefits of patterns

1. Consistency and reliability
2. Efficiency
3. Commonly understood taxonomy

# Pattern-based threat modelling approach – a solution to enable scalability

## Step 1- Identify commonly recurring patterns in applications

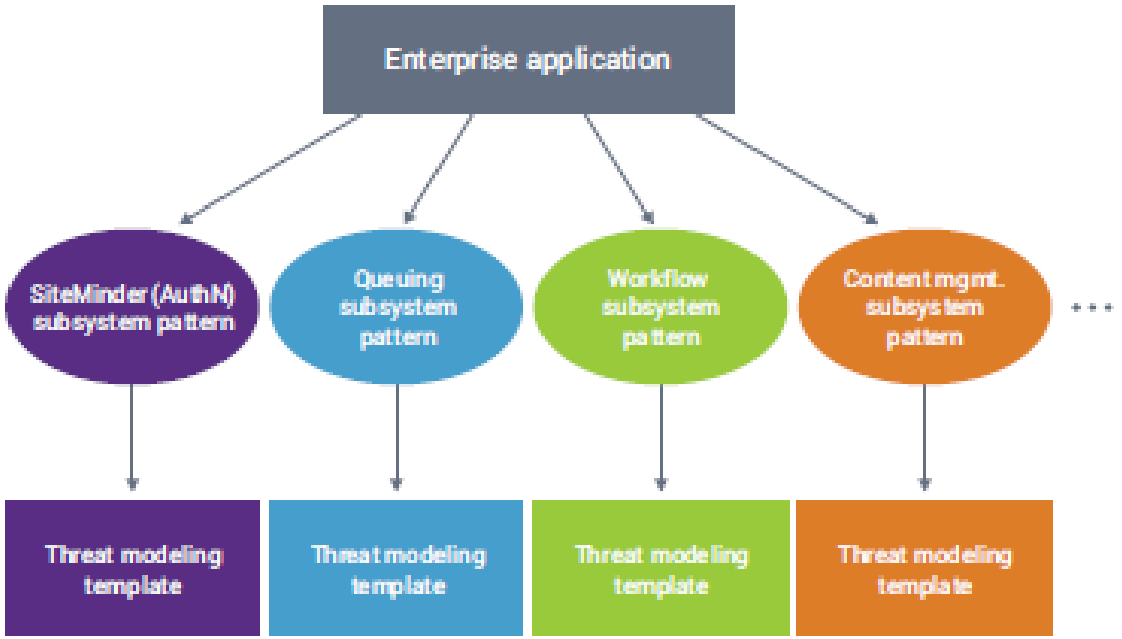



*Figure 1: Pattern-based approach to threat modeling*

# Step 2 – Create and maintain a pattern catalogue

Pattern catalogue contains the following information

- Pattern name
- Pattern description
- Threat modelling template associated with the pattern
- Applicability criteria

# Step 3 – Establish threat modelling templates

- Threat Name
- Threat description
  - Threat agents, assets, trust zones, etc.
  - A set of mitigating controls – for each control
    - ➢ security requirements
    - ➢ design guidance

# Step 3 – Establish threat modelling templates

- Threat Name
- Threat description
  - Threat agents, assets, trust zones, etc.
  - A set of mitigating controls – for each control
    - Security requirements
    - Design guidance
    - Development guidance
    - Testing guidance

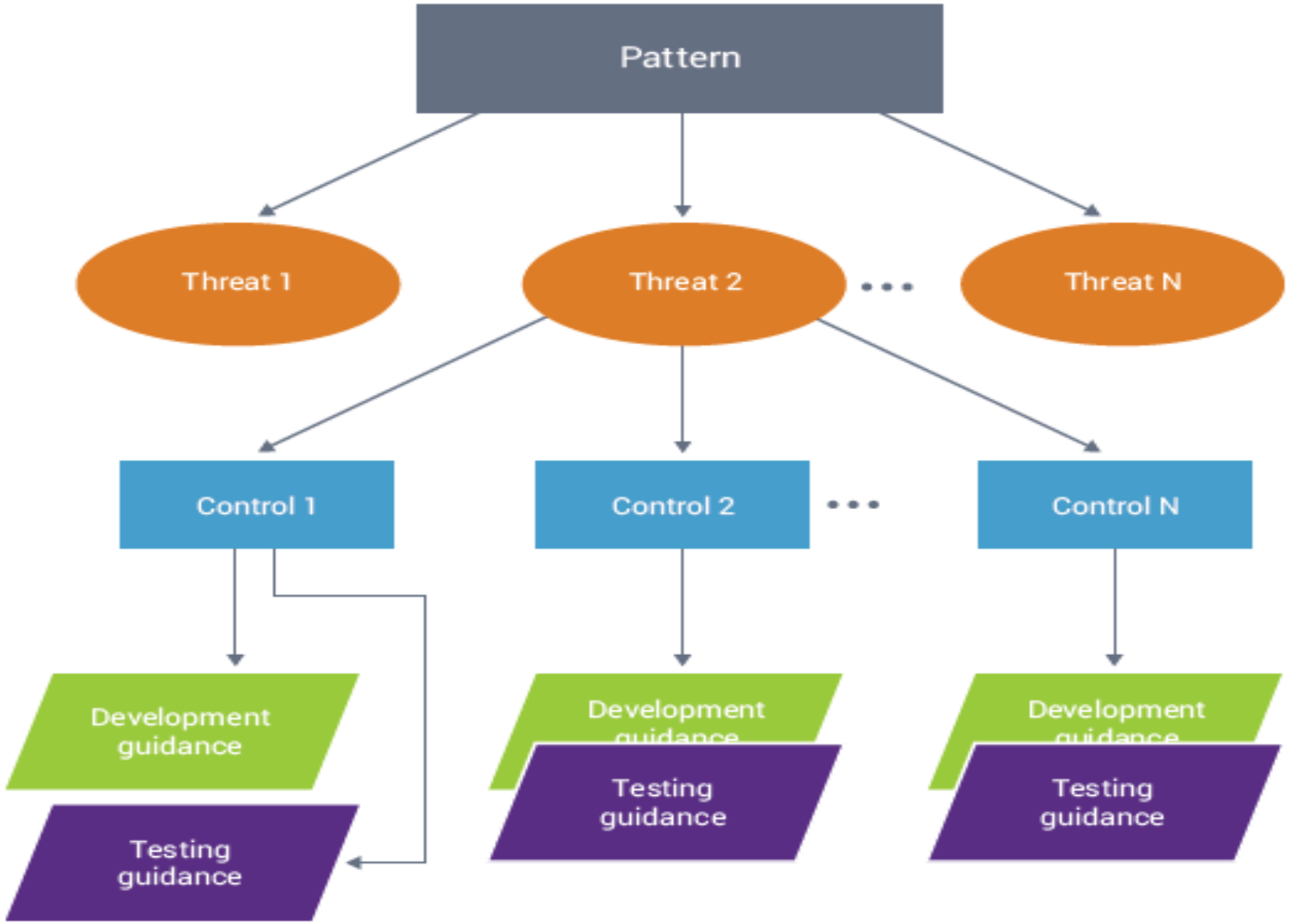
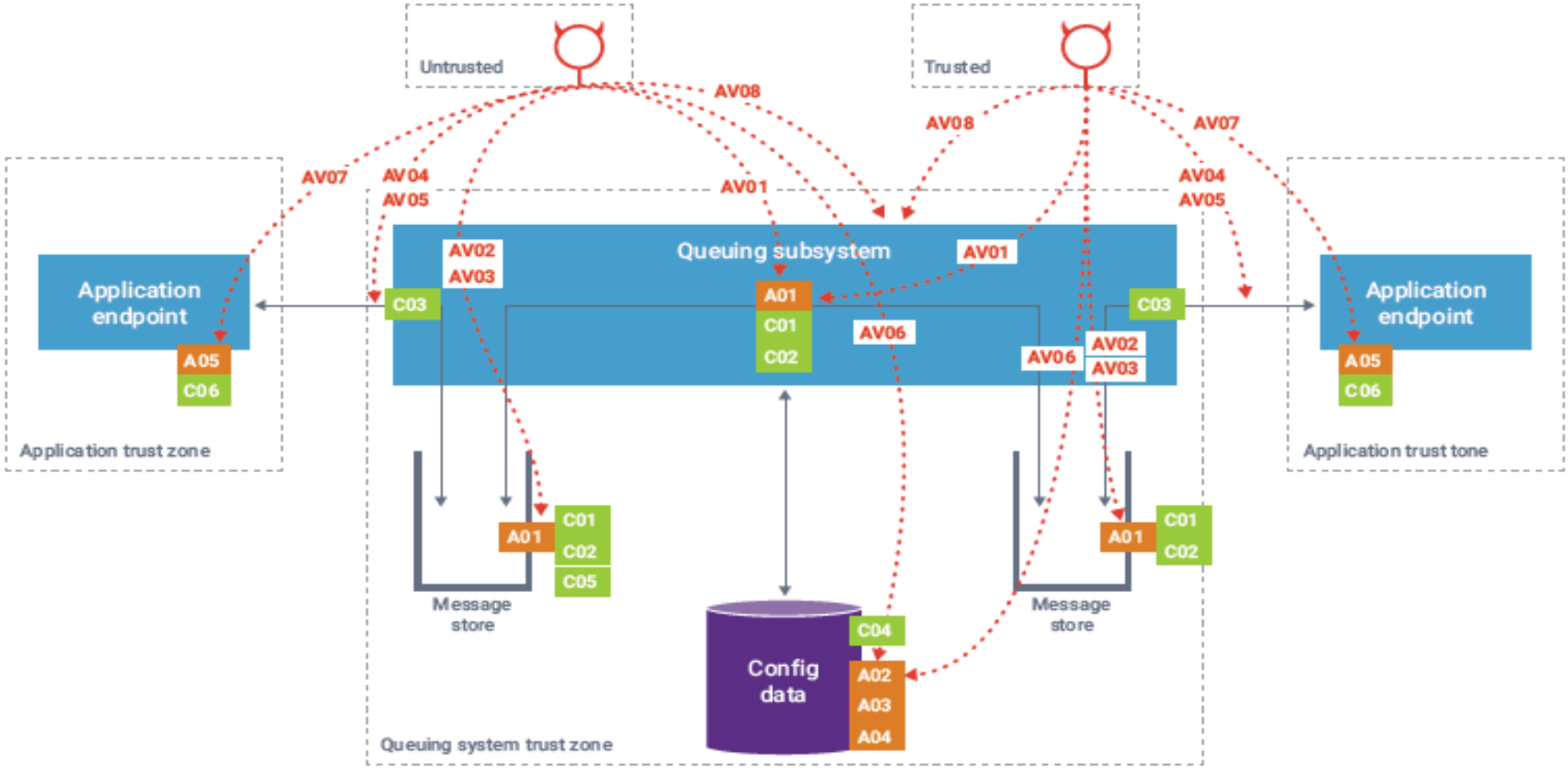



*Figure 2: Threat modeling template*

# Improve threat modelling process

1. Decompose an application and identify patterns in the application architecture
2. Use pattern-based template to arrive at a set of threats that must be considered during threat modelling process
3. Prioritize and prune the set of threats using organisation's risk framework when present, and using the applicability criteria in the template
4. Finalise the list of threats that must be considered for the analysis

# Sample threat model template for message queue pattern



| Assets | Required controls | Attack vectors |
| --- | --- | --- |
| A01: Messages<br>A02: Queue definitions<br>A03: User profiles<br>A04: Policy decision data<br>A05: Application configuration data to access queuing system | C01: Encryption of messages<br>C02: Integrity control on messages<br>C03: Queuing subsystem authentication control<br>C04: Database access control<br>C05: Message store access control<br>C06: Configuration data access control | AV01: Read/modify/tamper with messages in transit<br>AV02: Read messages in the message store<br>AV03: Modify messages in the message store<br>AV04: Unauthorized users publish messages<br>AV05: Unauthorized users receive messages<br>AV06: Unauthorized access to the queuing system's administrative interface<br>AV07: Compromised queuing system authentication credentials<br>AV08: Denial-of-service attack on the queuing system |