National Mining University
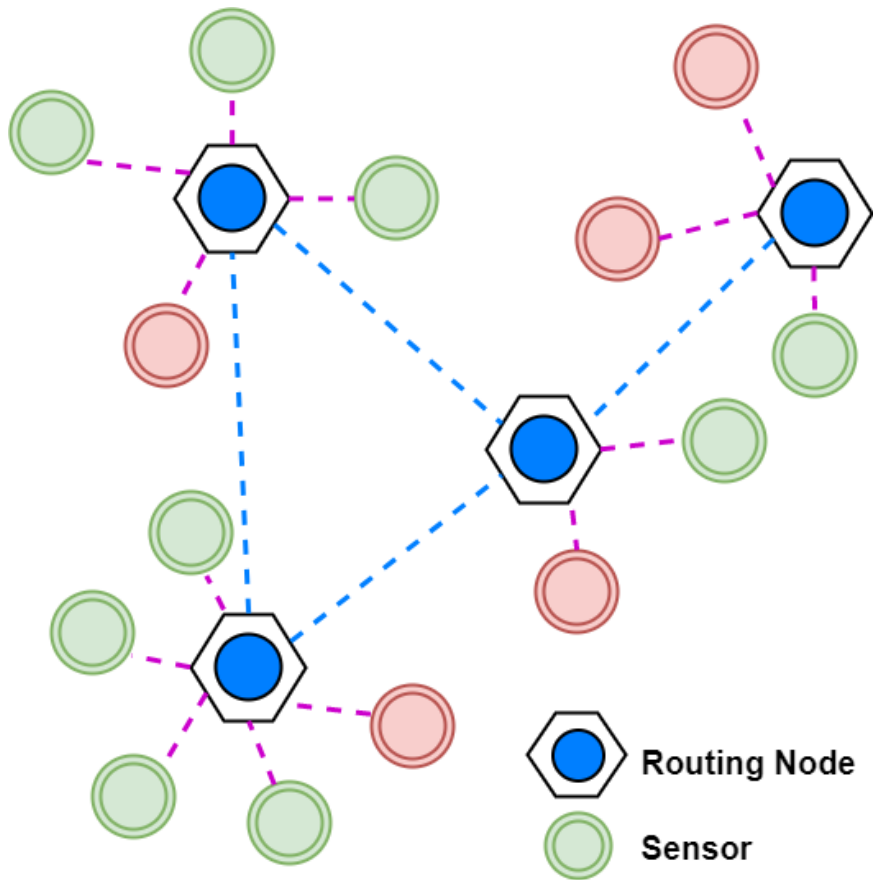
PROTECTION OF INFORMATION IN COMMUNICATION NETWORKS

authors:
Yuliia Kovalova
Vadym Mieshkov

Dnipro, Ukraine
2017

**Routing Node**

Sensor

Wireless sensor networks have found many applications and play an important role in infrastructure monitoring.

The use of wireless technology provides many benefits from the increased availability of information resources, and the popularity of sensor networks is associated with the ability to work autonomously without the help of any infrastructure or interaction with a person.

However, wireless technology and the autonomy of sensor networks generate new threats and increases the risk of information security.

2

Internet of Things (IoT)
Types of wireless networks
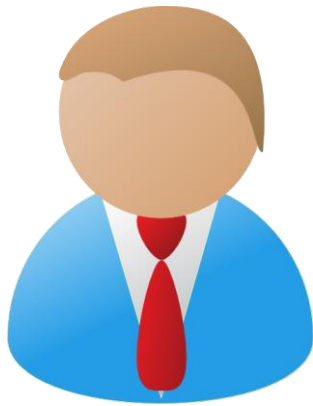
| Personal	Local	Global
WPAN	WLAN	Cellular (2G, 3G, 4G-LTE)

Internet of Things (IoT) LoRaWAN™

LoRaWAN™ is a Low Power Wide Area Network (LPWAN) specification intended for wireless battery operated Things in a regional, national or global network. LoRaWAN targets key requirements of Internet of Things such as secure bi-directional communication, mobility and localization services. The LoRaWAN specification provides seamless interoperability among smart Things without the need of complex local installations and gives back the freedom to the user, developer, businesses enabling the roll out of Internet of Things.
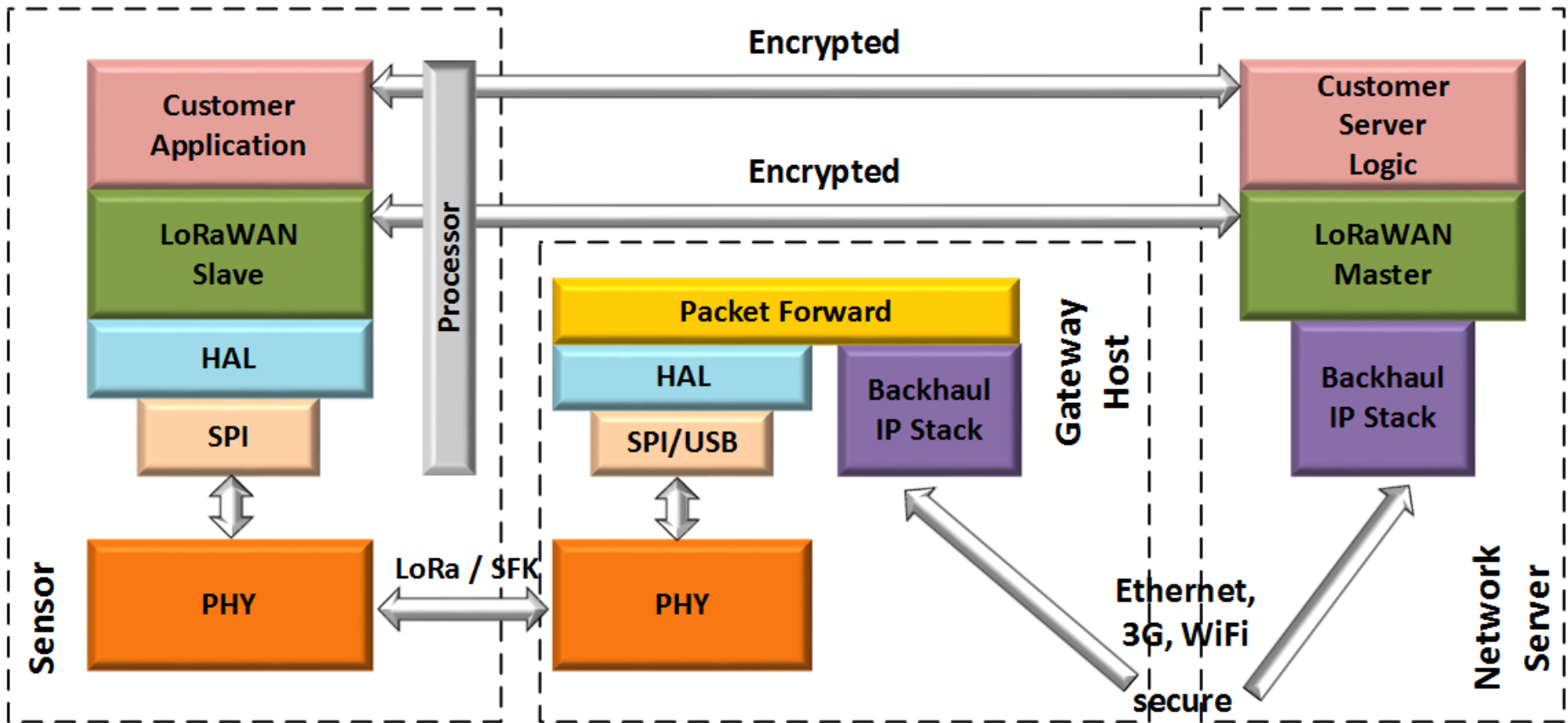
- **LoRaWAN** network architecture is typically laid out in a star-of-stars topology in which gateways is a transparent bridge relaying messages between end-devices and a central network server in the backend.

Internet of Things (IoT) ZigBee

Zigbee Smart Energy is the world's leading standard for interoperable products that monitor, control, inform, and automate the delivery and use of energy and water. It is used to deliver innovative solutions for smart meters and the home area network (HAN) that allow consumers to know and control their energy use by connecting them to the smart grid and helps create greener homes by giving consumers the information and automation needed to easily reduce their consumption and save money.

6

- **ZigBee** is an IEEE 802.15.4-based specification for high-level communication protocols.
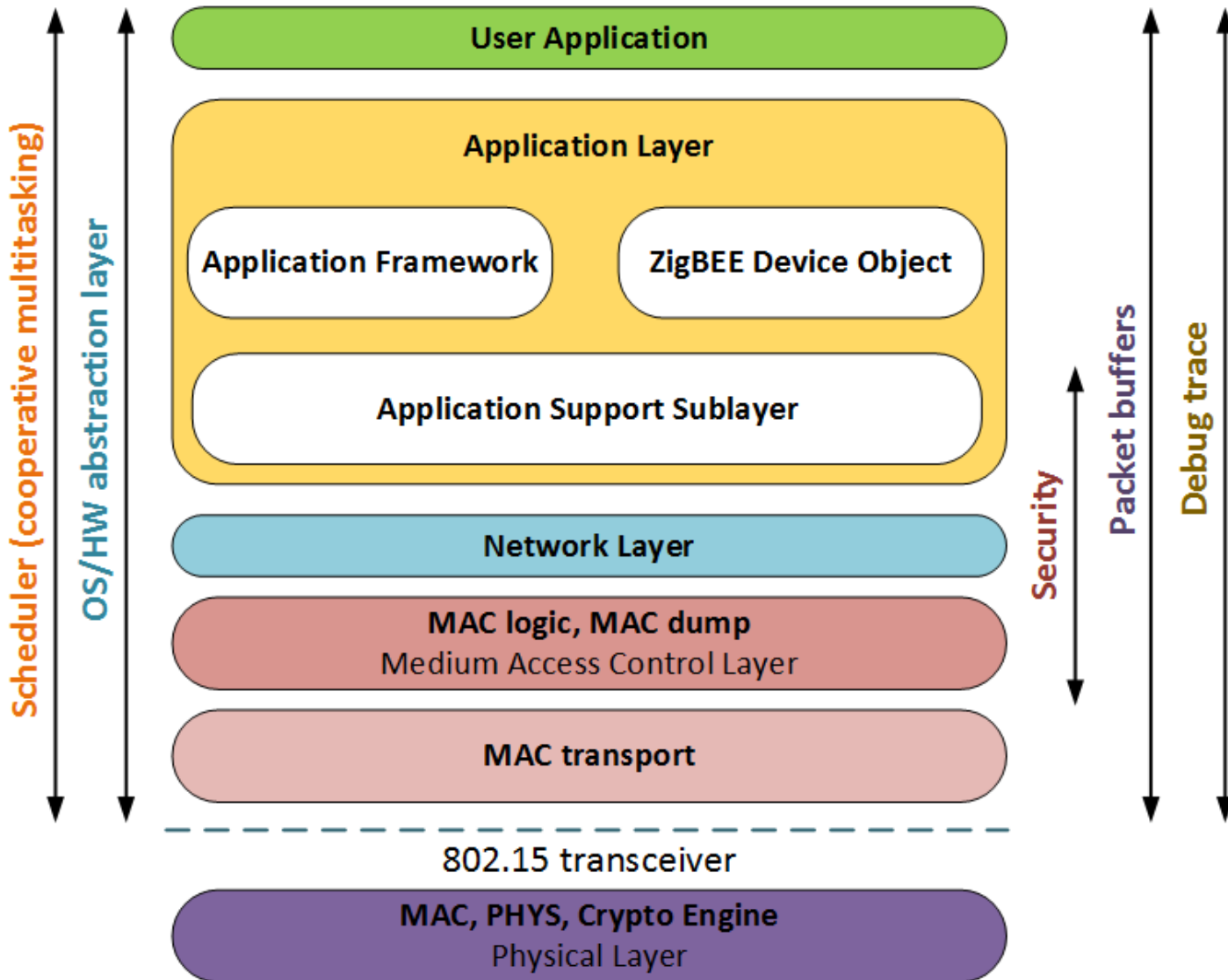
In recent years, the rise in the number of cyber attacks has been on the plug-in user devices related to the Internet of Things (IoT). These devices are vulnerable to cyber attacks because they are not equipped with basic security features. The use of IoT devices for DDoS attacks is an accomplished fact.

Wireless technology and autonomy of sensor networks generate new threats and increases the risk of information security. Inadequate physical and cryptographic protection makes them sensitive to interception, compromise and hacking. As a result, any encrypted data contained in these networks can be exploited by malicious people to commit attacks from the network, compromising the confidentiality of information.

Problems of safety of data networks

- Database management systems and IT infrastructure are the most critical from the point of view of cybernetic security. Cybernetic security is the most important component of a constantly developing modern network.

- Distribution of public "cloud" services is hampered not by security considerations, but by the need to comply with regulatory and legislative requirements.

- The Cloud Security Alliance has released a package of free programs called Governance, Risk Management and Compliance Stack, which allows many government requirements to be met.

- Cloud infrastructure can eliminate technological fragmentation, simplify IT management, make the most of existing investments in installed equipment and technologies, and increase the efficiency of business processes in energy companies.

- the design of the information security system ***should be carried out at the stage of the technical task for building the system***, since the success of any hacker attack is related to the vulnerability of the devices and their operating system, and not the applications installed on these devices.

- In this regard, the **most urgent task of designing in-house and local networks of municipal monitoring**, operating on unlicensed frequencies of the IMS (868 MHz and 2.4 GHz) band using **LoRa and ZigBee technologies**, is to ***encapsulate protected proprietary protocols into existing stacks.***

Thank you for your attention!