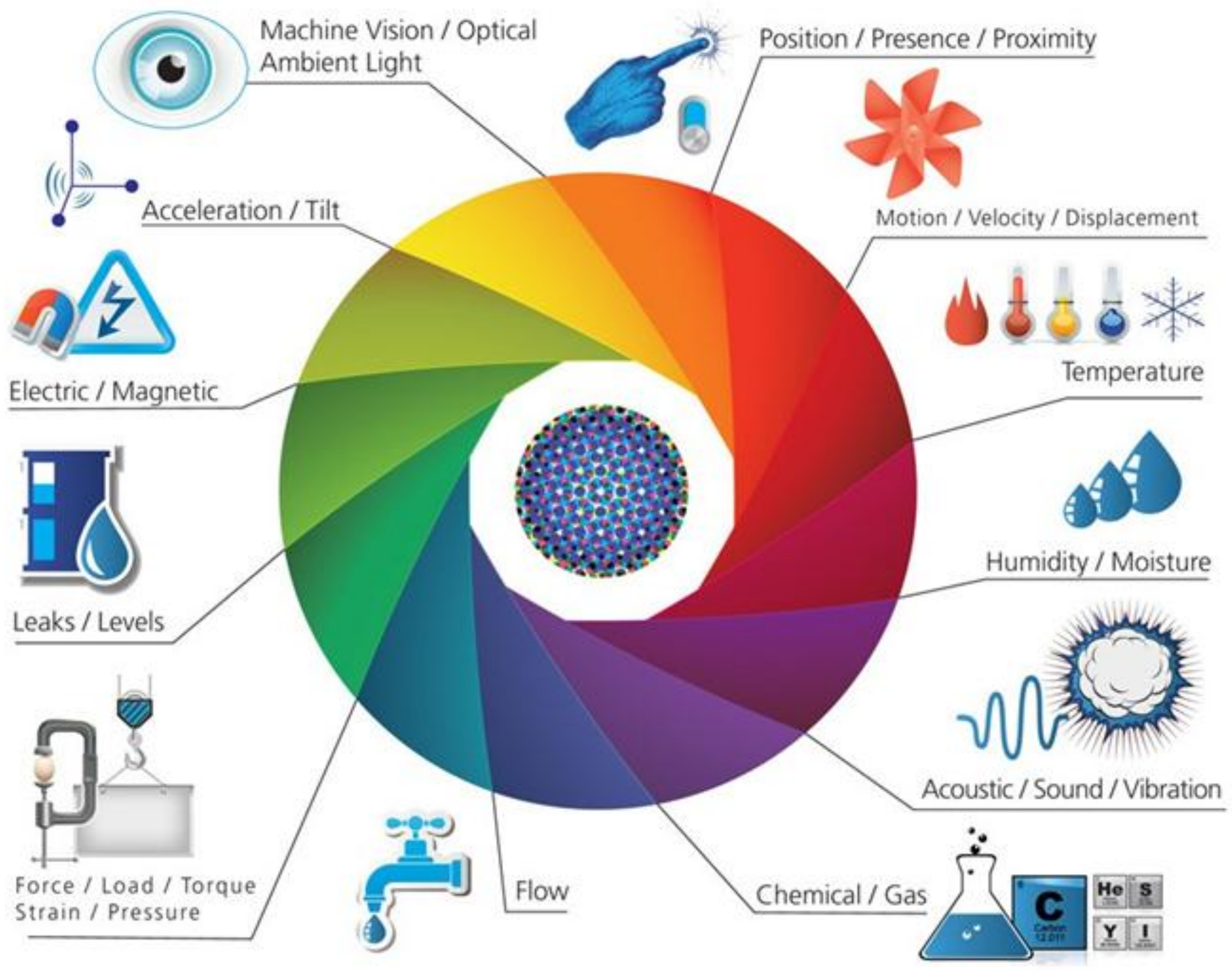
Analysis of attacks on components of IoT systems and cybersecurity technologies

Nadiia M.Lobanchykova,
Zhytomyr Polytechnic State University, Ukraine
Ihor A.Pilkevych and
S.P.Korolev Zhytomyr Military Institute, Ukraine
Oleksandr Korchenko
University of Bielsko-Biala, Poland



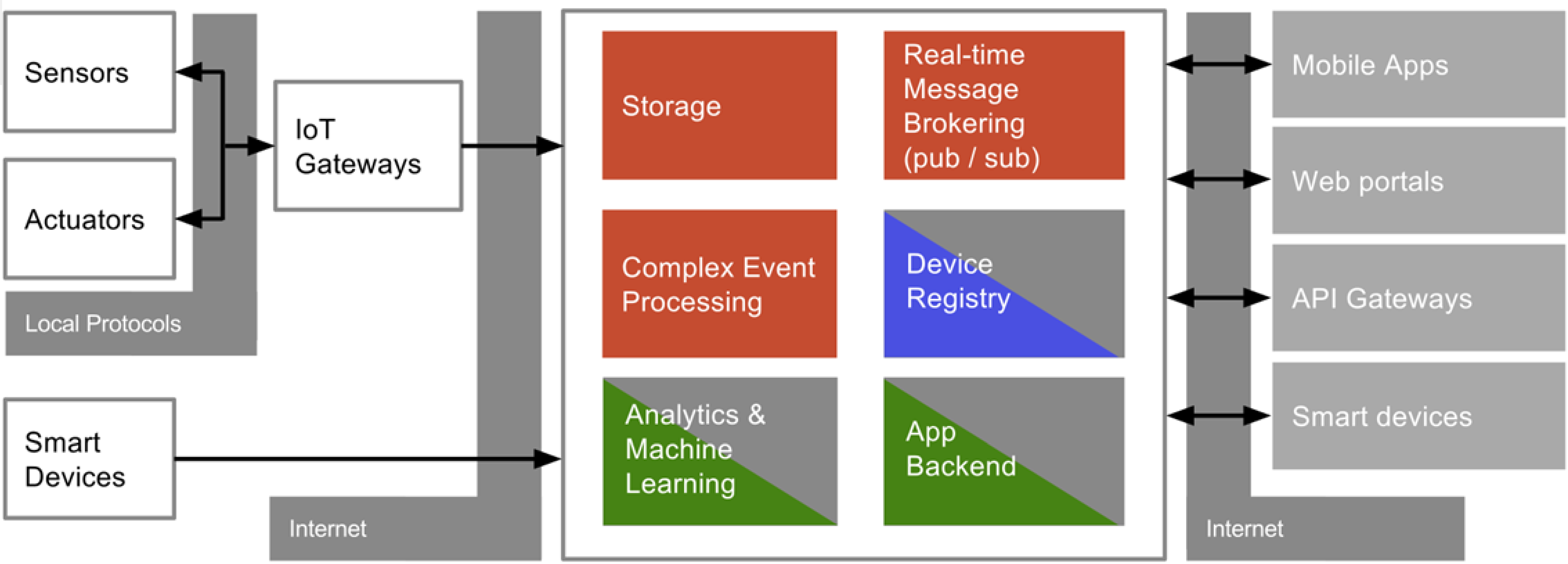
Machine Vision / Optical
Ambient Light
Position / Presence / Proximity
Acceleration / Tilt
Motion / Velocity / Displacement
Electric / Magnetic
Temperature
Humidity / Moisture
Leaks / Levels
Acoustic / Sound / Vibration
Force / Load / Torque
Strain / Pressure
Flow
Chemical / Gas
C
He
S
Y
I

6,3 billion	6,8 billion	7,2 billion	7,6 billion	world population
500 million	12,5 billion	25 billion	50 billion	number of connected devices
2003	2010	2015	2020	
0,8	1,84	3,47	6,58	number of connected devices per person

Edge

Event processing, Analytics

Applications



Sensors

Actuators

Local Protocols

IoT Gateways

Smart Devices

Internet

Storage

Real-time Message Brokering (pub / sub)

Complex Event Processing

Device Registry

Analytics & Machine Learning

App Backend

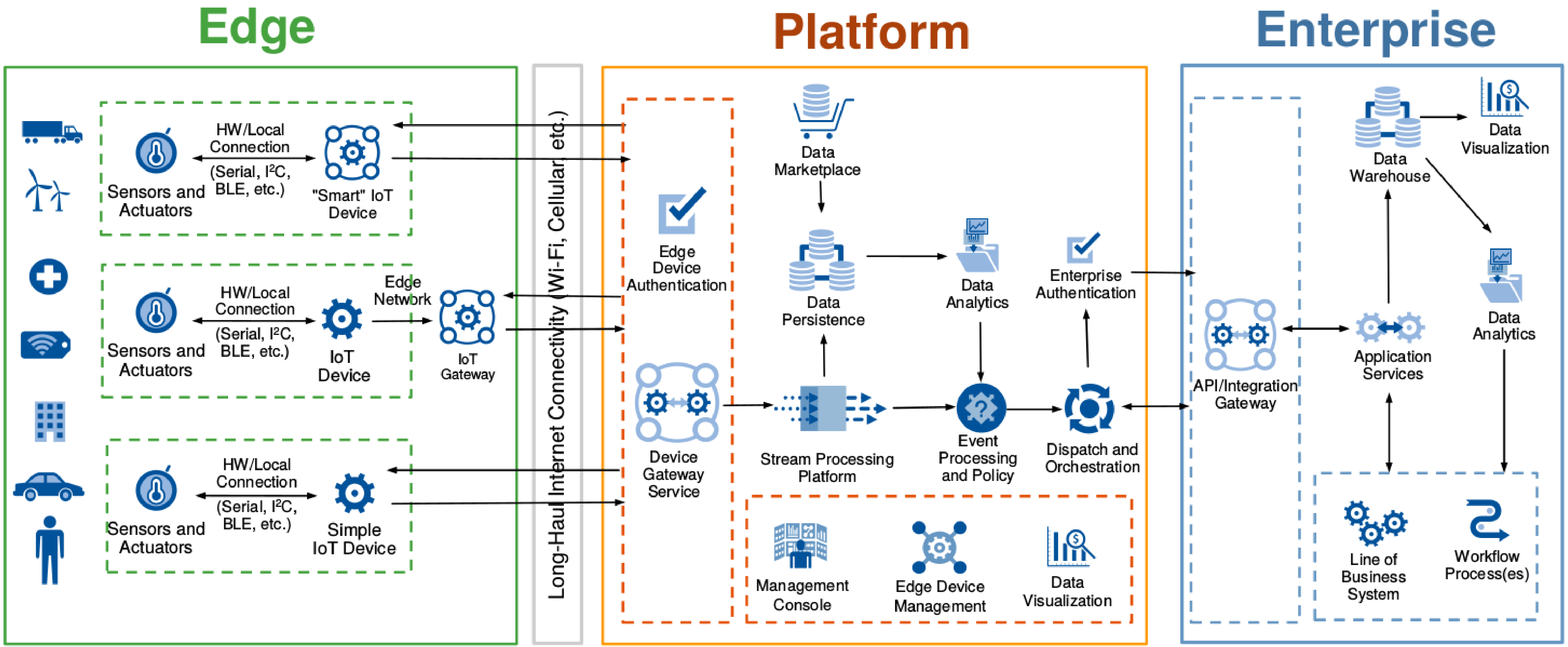
Internet

Mobile Apps

Web portals

API Gateways

Smart devices



Edge

Sensors and Actuators

HW/Local Connection

(Serial, I^{2}C, BLE, etc.)

"Smart" IoT Device

Sensors and Actuators

HW/Local Connection

(Serial, I^{2}C, BLE, etc.)

IoT Device

Edge Network

IoT Gateway

Sensors and Actuators

HW/Local Connection

(Serial, I^{2}C, BLE, etc.)

Simple IoT Device

Long-Haul Internet Connectivity (Wi-Fi, Cellular, etc.)

Platform

Edge Device Authentication

Device Gateway Service

Data Marketplace

Data Persistence

Data Analytics

Enterprise Authentication

Stream Processing Platform

Event Processing and Policy

Dispatch and Orchestration

Management Console

Edge Device Management

Data Visualization

Enterprise

API/Integration Gateway

Data Warehouse

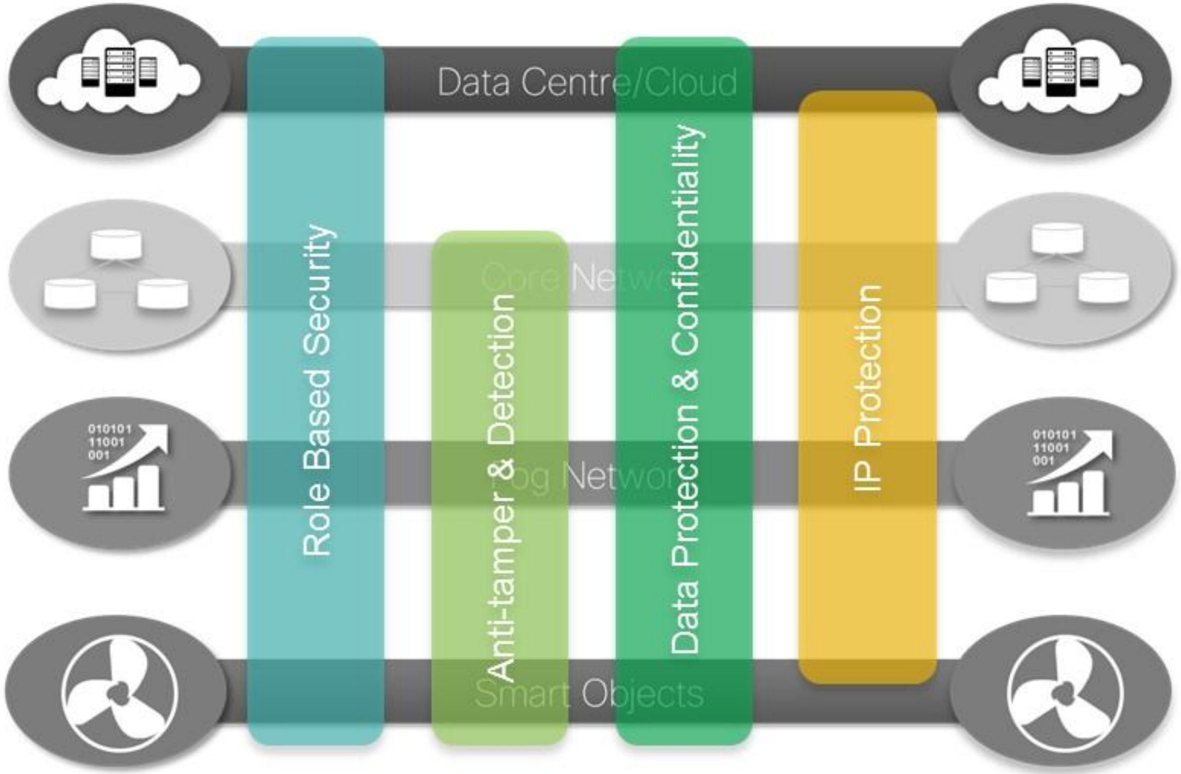
Data Visualization

Data Analytics

Application Services

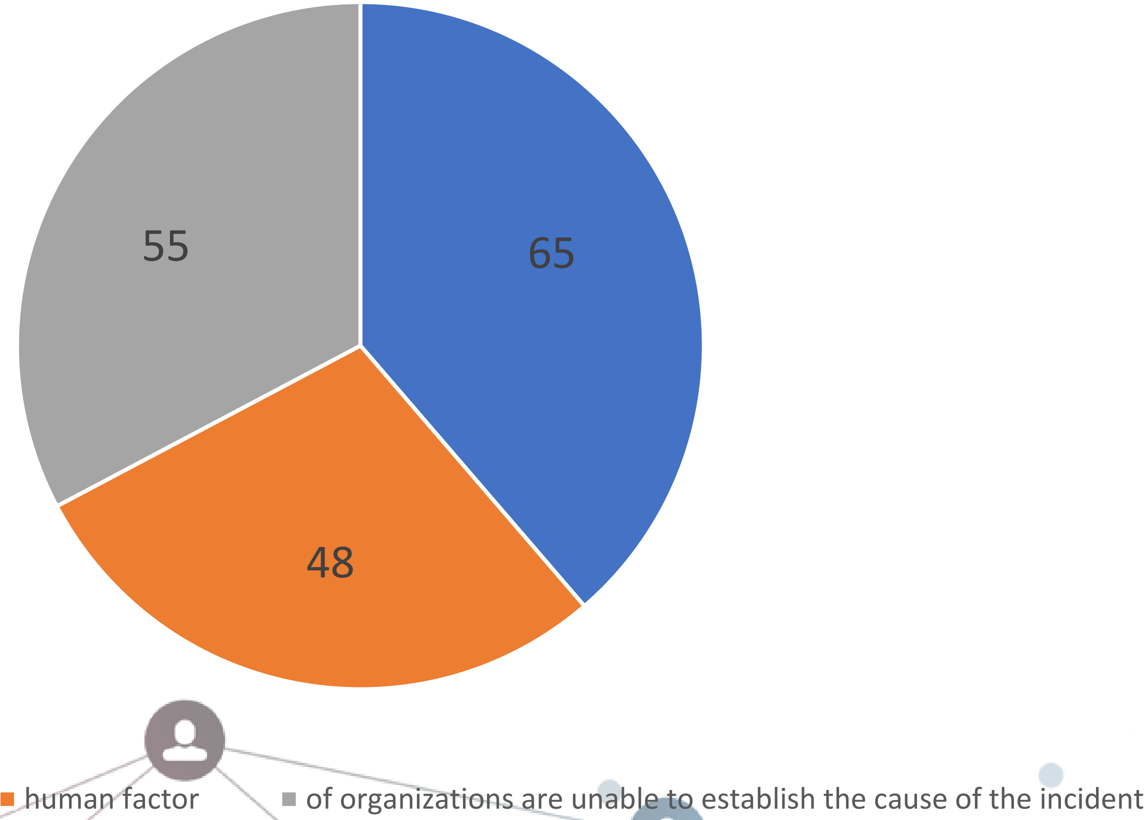
Line of Business System

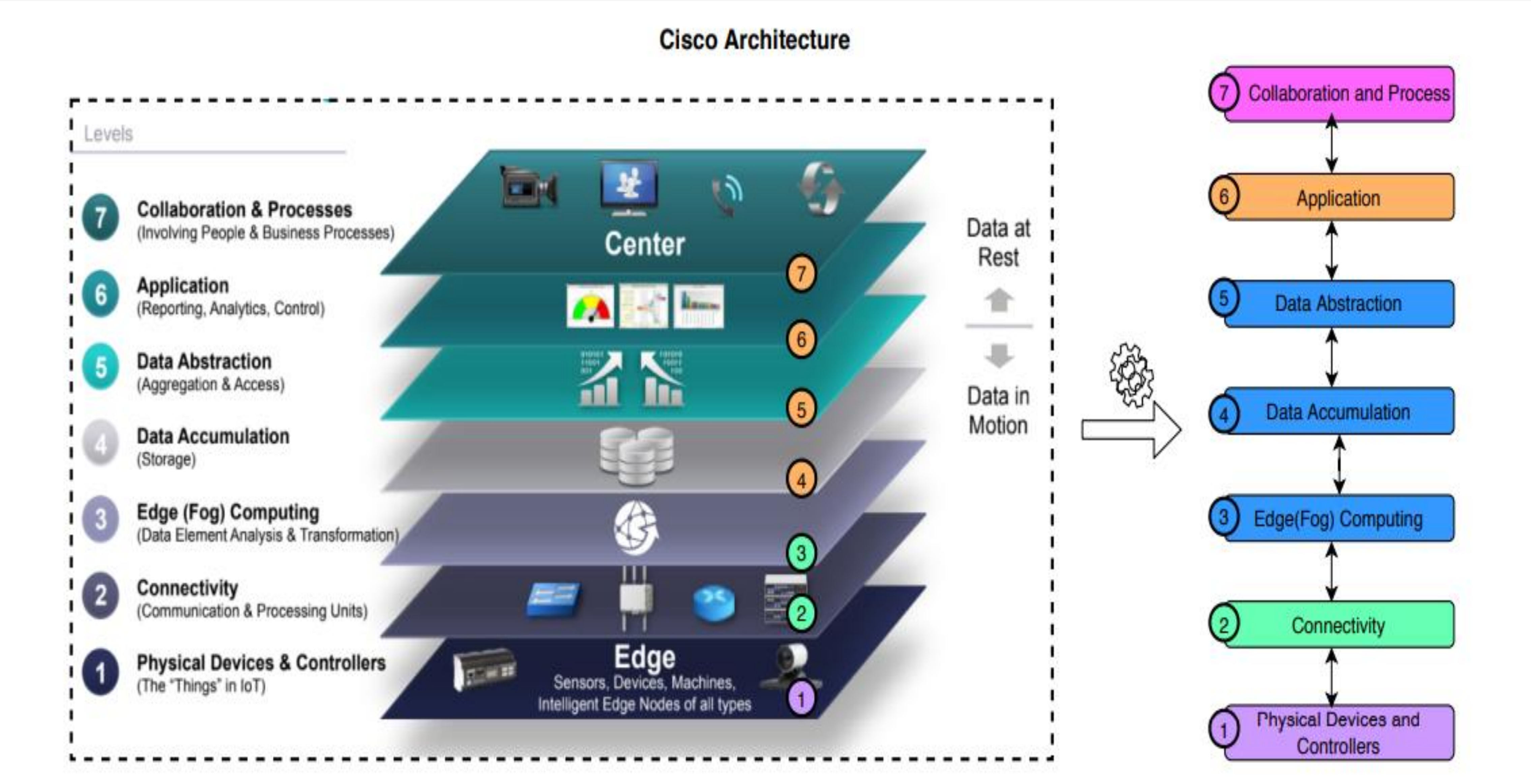
Workflow Process(es)



- Dynamic distributed intelligence
- Distributed Analytics & Management
- Network Enforcement/Segmentation
- Authenticated Encryption
- Connectivity Standards
- Stateful application visibility
- Auto enrolment & Provisioning
- Device Classification
- Standards for actuator & Sensors

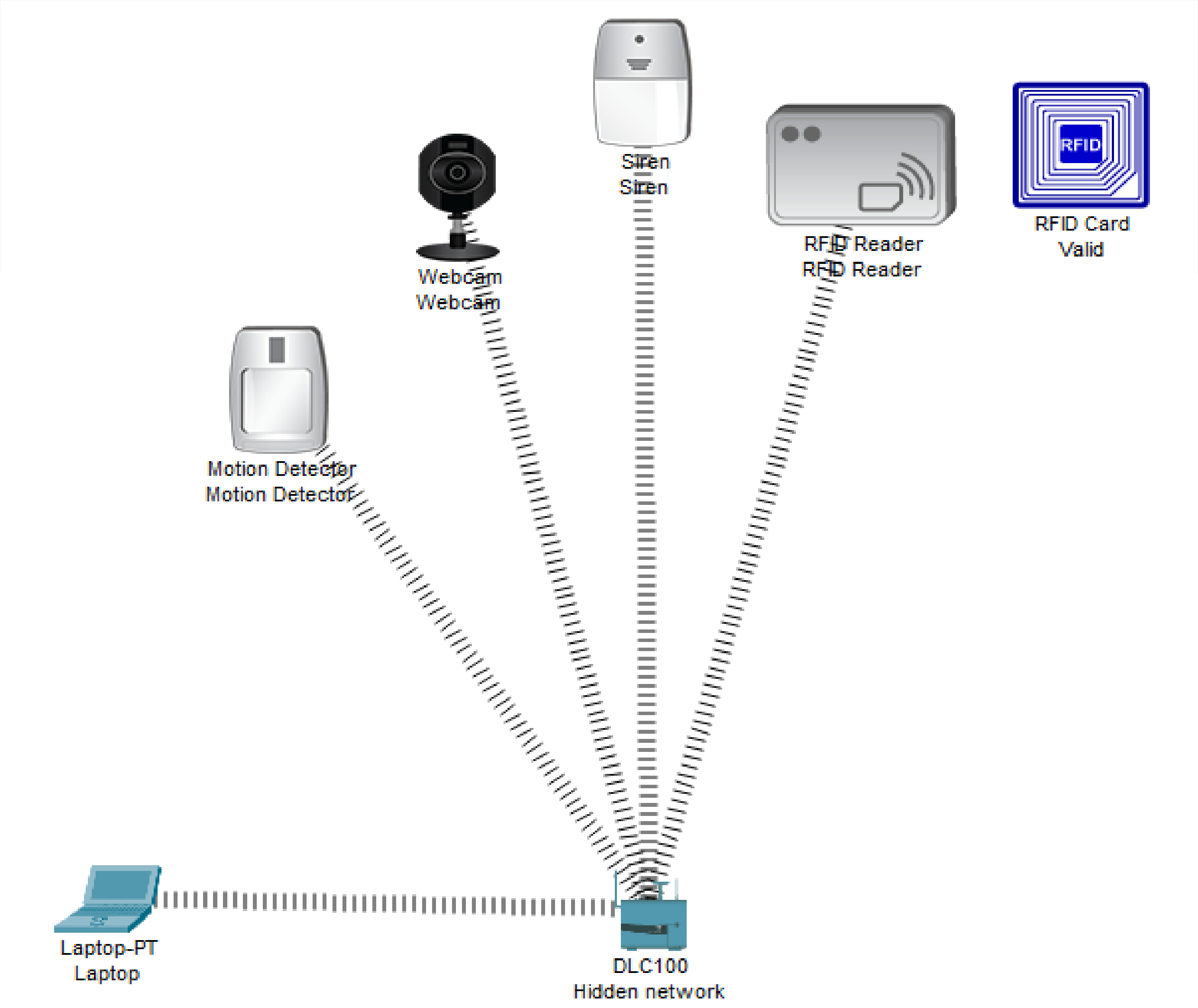
Global statistics compiled by Cisco in 2017



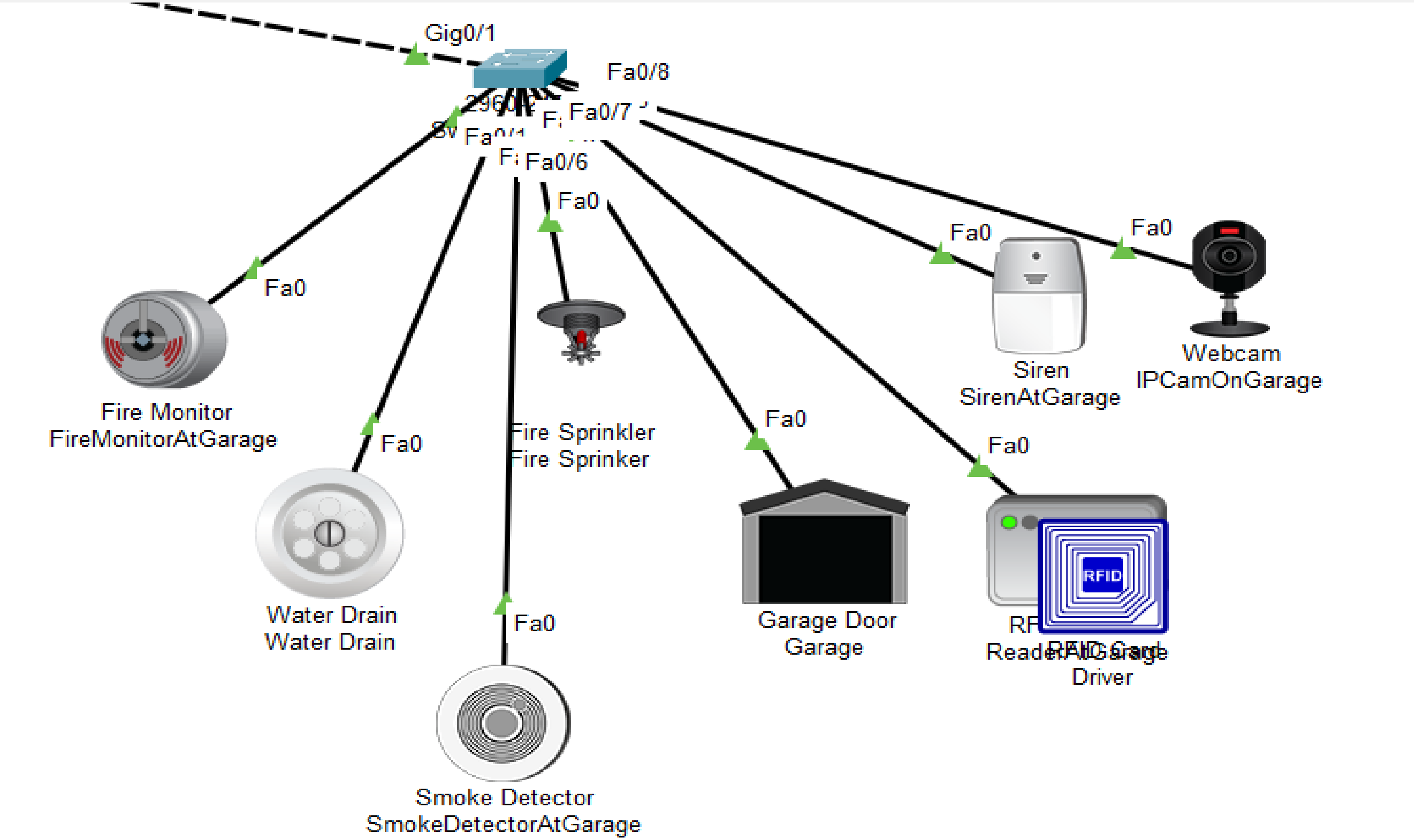

Cisco Architecture
Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge (Fog) Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types
7
6
5
4
3
2
1
Data at Rest
Data in Motion
7 Collaboration and Process
6 Application
5 Data Abstraction
4 Data Accumulation
3 Edge(Fog) Computing
2 Connectivity
1 Physical Devices and Controllers

We choose the 7-level architecture of IoT systems, proposed by Cisco

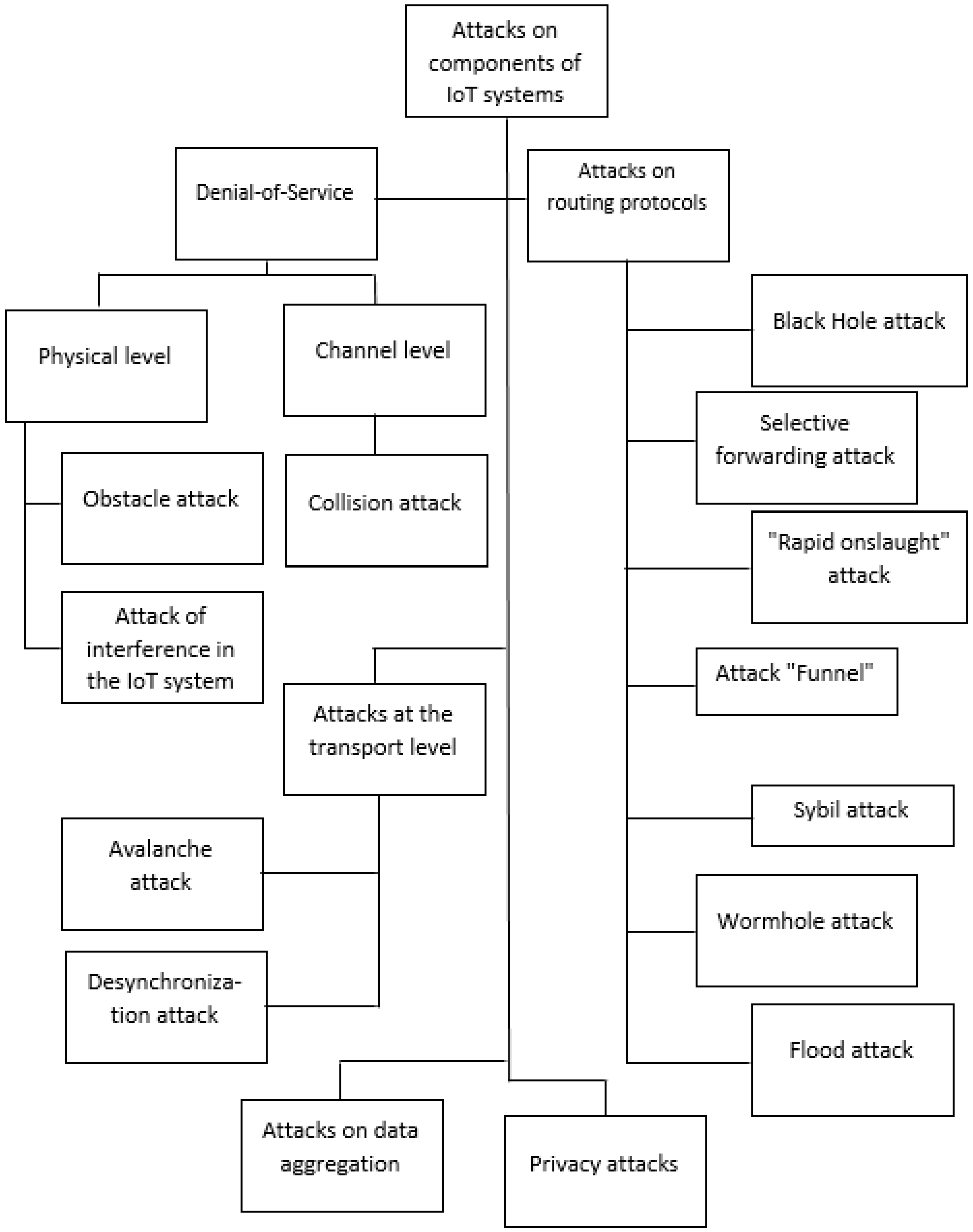
Cluster protection zone



Scheme of fire alarm system of a separate room on the example of a garage



Attacks on IoT system components


Attacks on components of IoT systems
Denial-of-Service
Attacks on routing protocols
Physical level
Channel level
Obstacle attack
Collision attack
Attack of interference in the IoT system
Black Hole attack
Selective forwarding attack
"Rapid onslaught" attack
Attack "Funnel"
Attacks at the transport level
Avalanche attack
Desynchroniza-tion attack
Sybil attack
Wormhole attack
Flood attack
Attacks on data aggregation
Privacy attacks

Attacks can be represented in the form of open classification groups.

$D = H \bigcup C$ - a set of attacks that lead to denials of service, involves combining sets of attacks at the physical and channel level.

Many attacks that lead to denials of service at the physical level:

$$H = \bigcup_{i=1}^{n} H_i$$

The set of attacks that lead to denial of service link-level:

$$C = \bigcup_{k=1}^{z} C_k$$

The set of attacks on routing protocols:

$$R = \bigcup_{v=1}^{s} R_v$$

The open classification grouping of transport layer attacks is presented in the form of a set:

$$T = \bigcup_{\alpha=1}^{l} T_\alpha$$

The set of attacks on data aggregation is represented as follows:

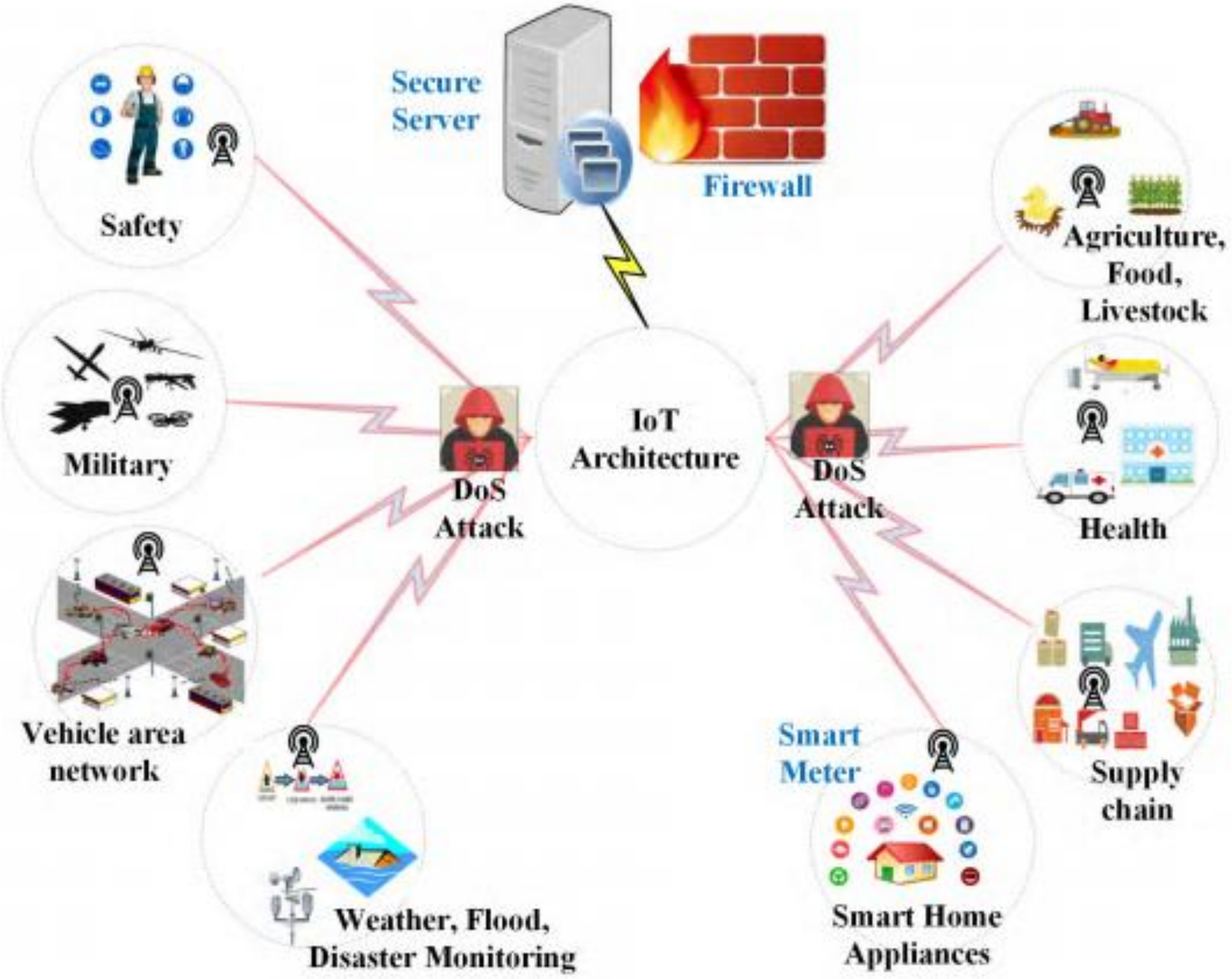
$$G = \bigcup_{j=1}^{m} G_j$$

The set of attacks on privacy:

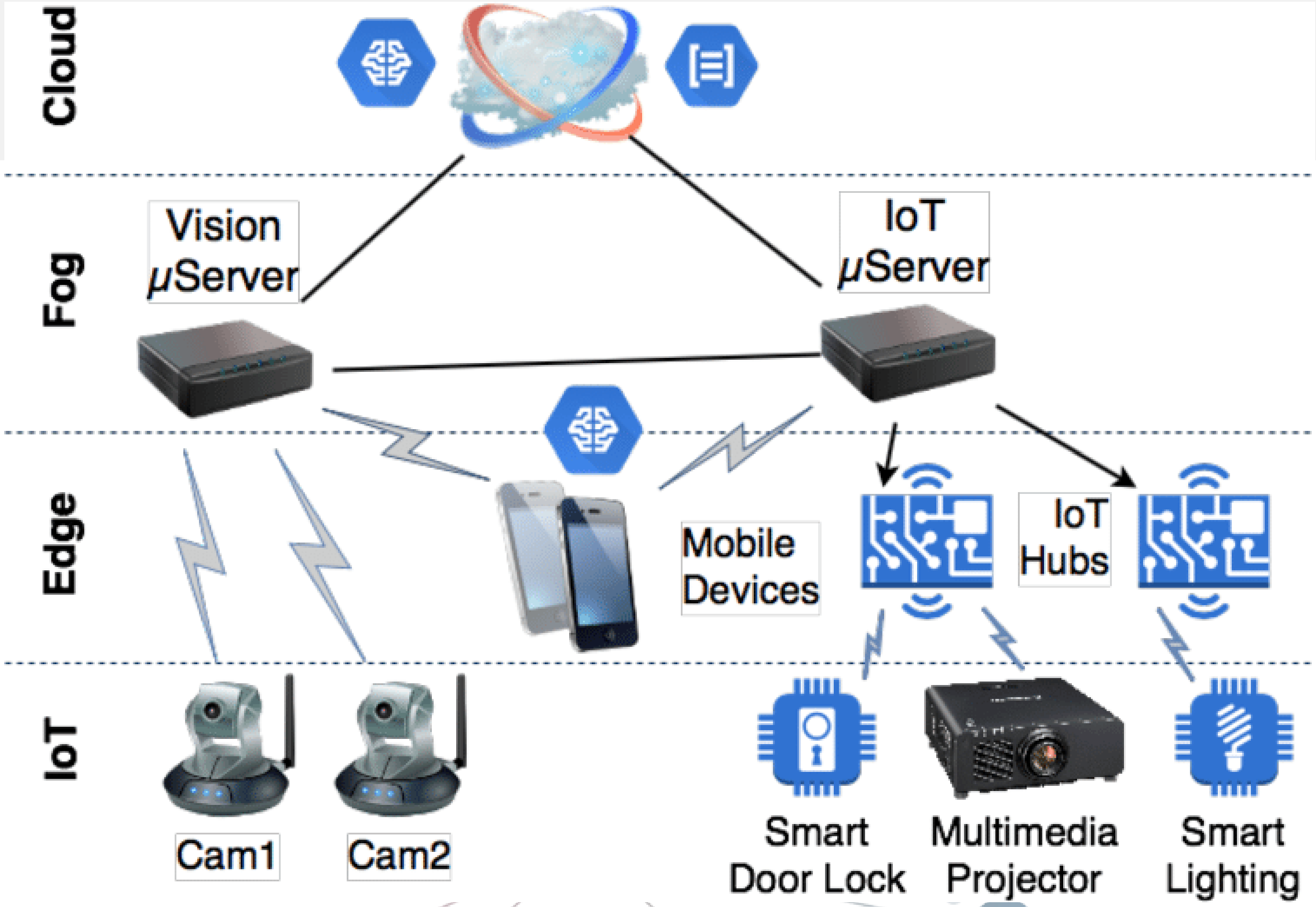
$$P = \bigcup_{\gamma=1}^{\delta} P_\gamma$$

In general, attacks can be represented as a union of all classification groups:

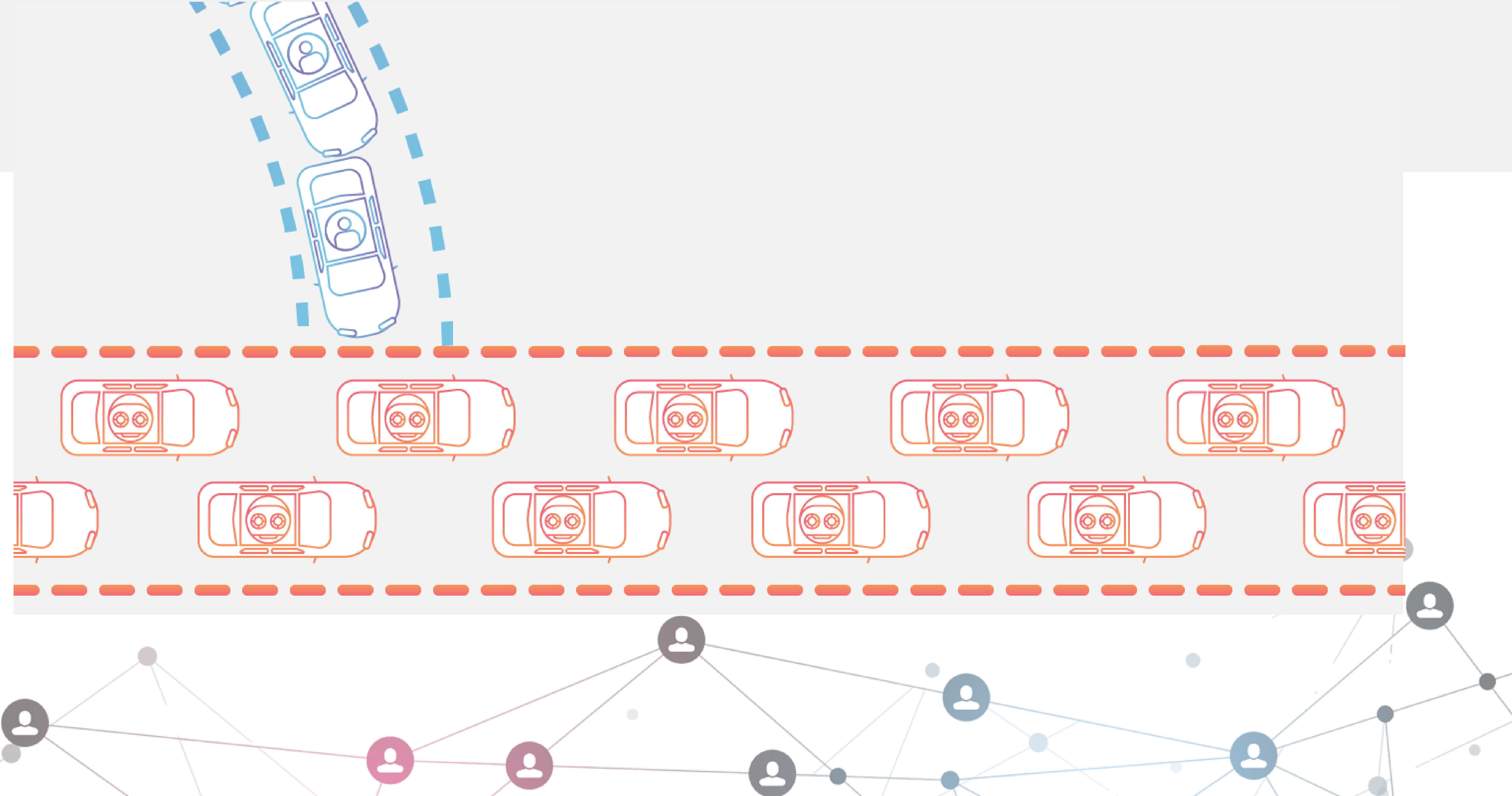
$A = D \bigcup R \bigcup T \bigcup G \bigcup P$

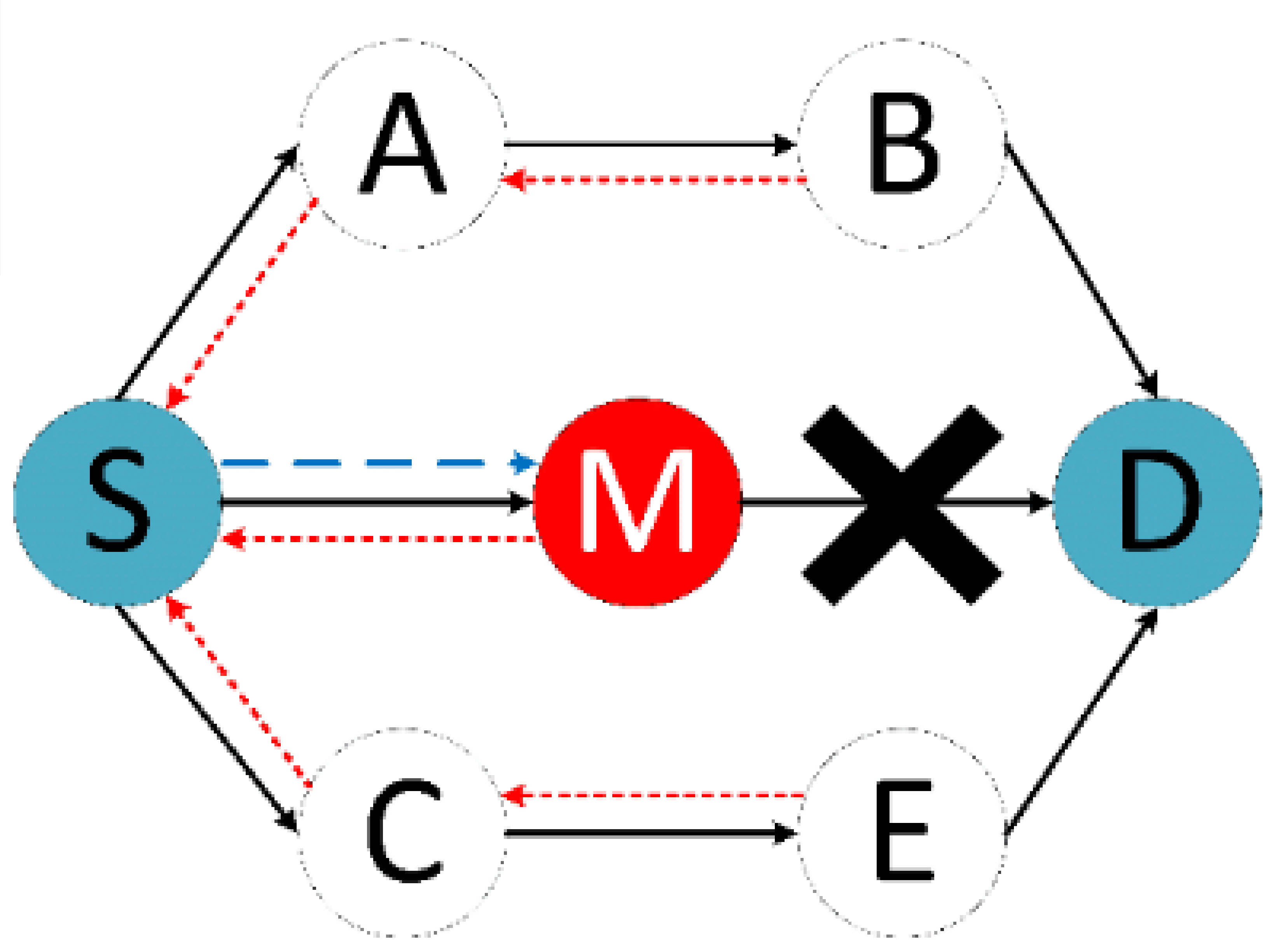

Secure Server
Firewall
Safety
Agriculture, Food, Livestock
Military
DoS Attack
IoT Architecture
DoS Attack
Health
Vehicle area network
Supply chain
Smart Meter
Weather, Flood, Disaster Monitoring
Smart Home Appliances

An attack on the IoT systems detection of a sensor



DoS channel level attack.



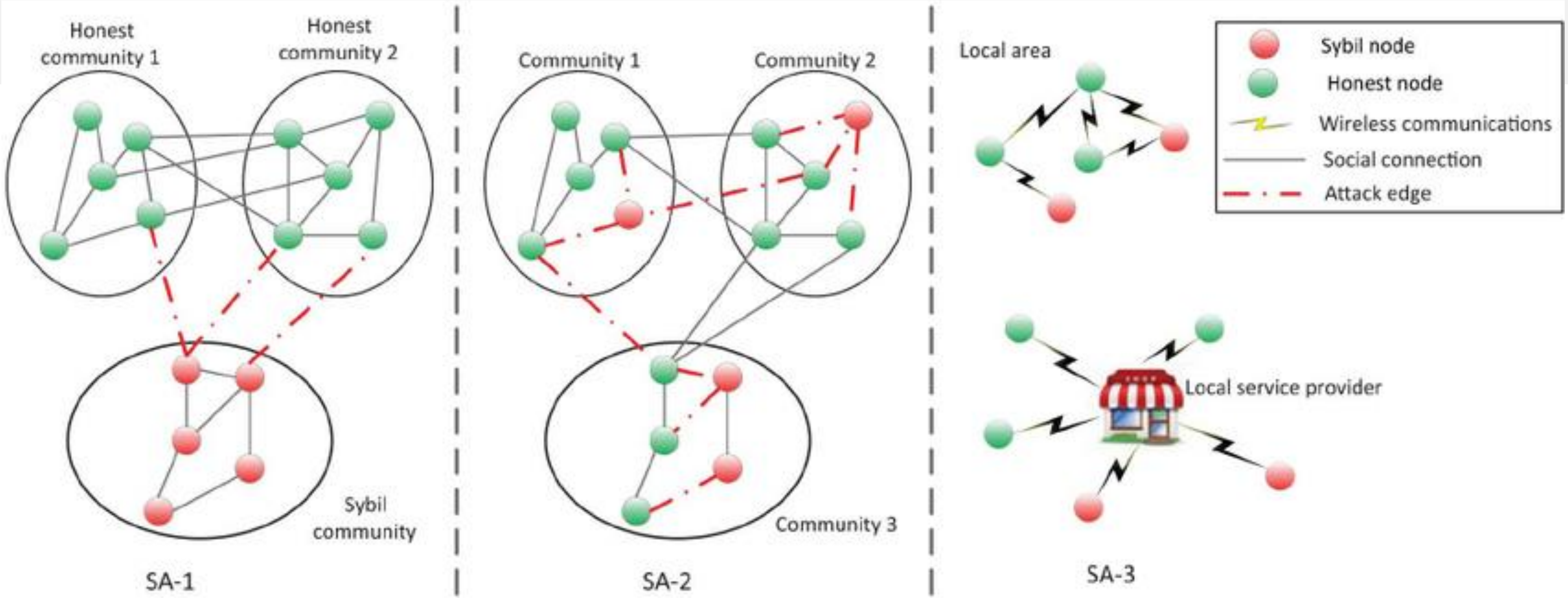


Black Hole attack

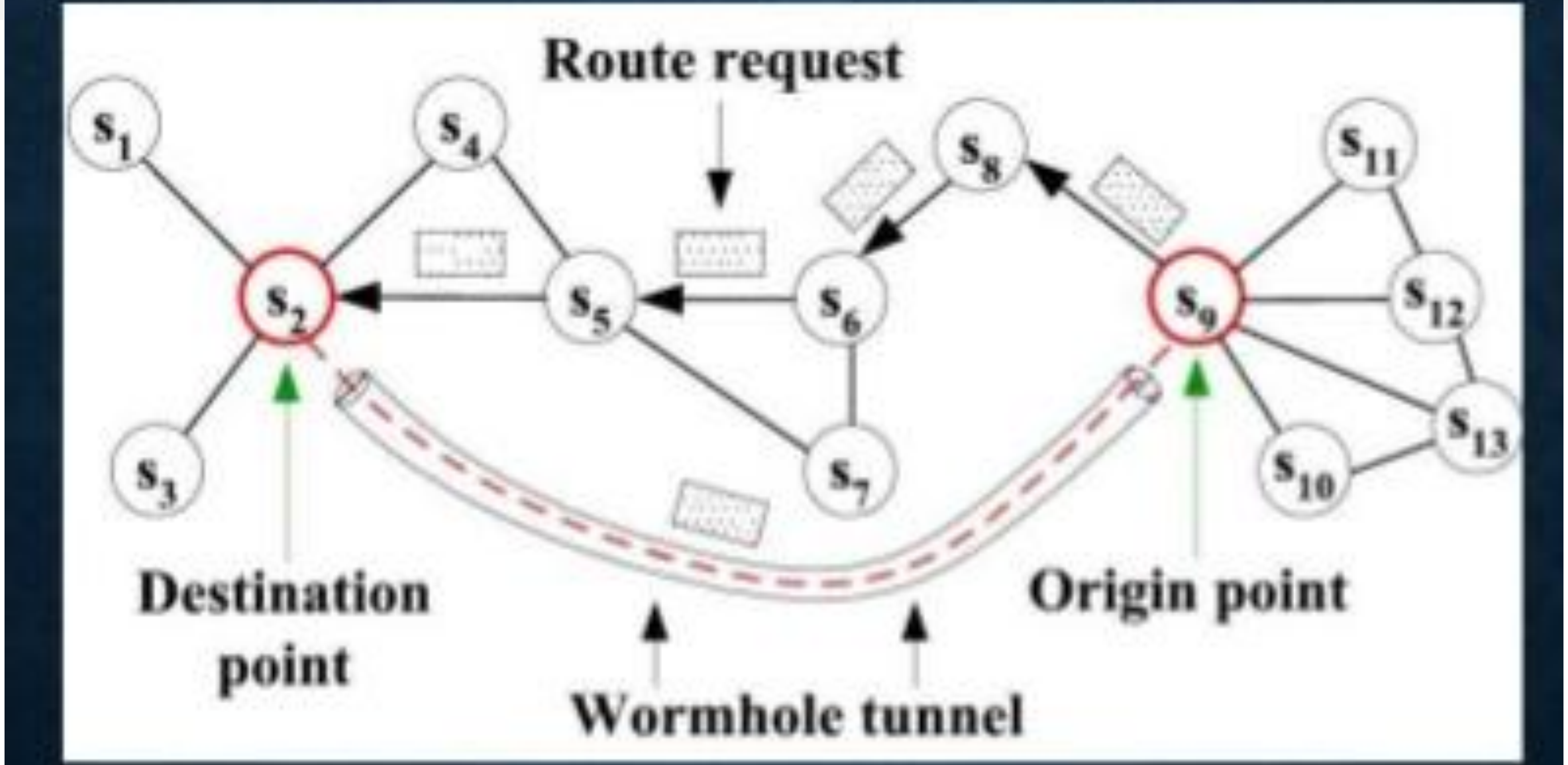
The "Funnel" attack

<svg onload=alert
<script>alert(1)</sc
e/onload=alert(1)>

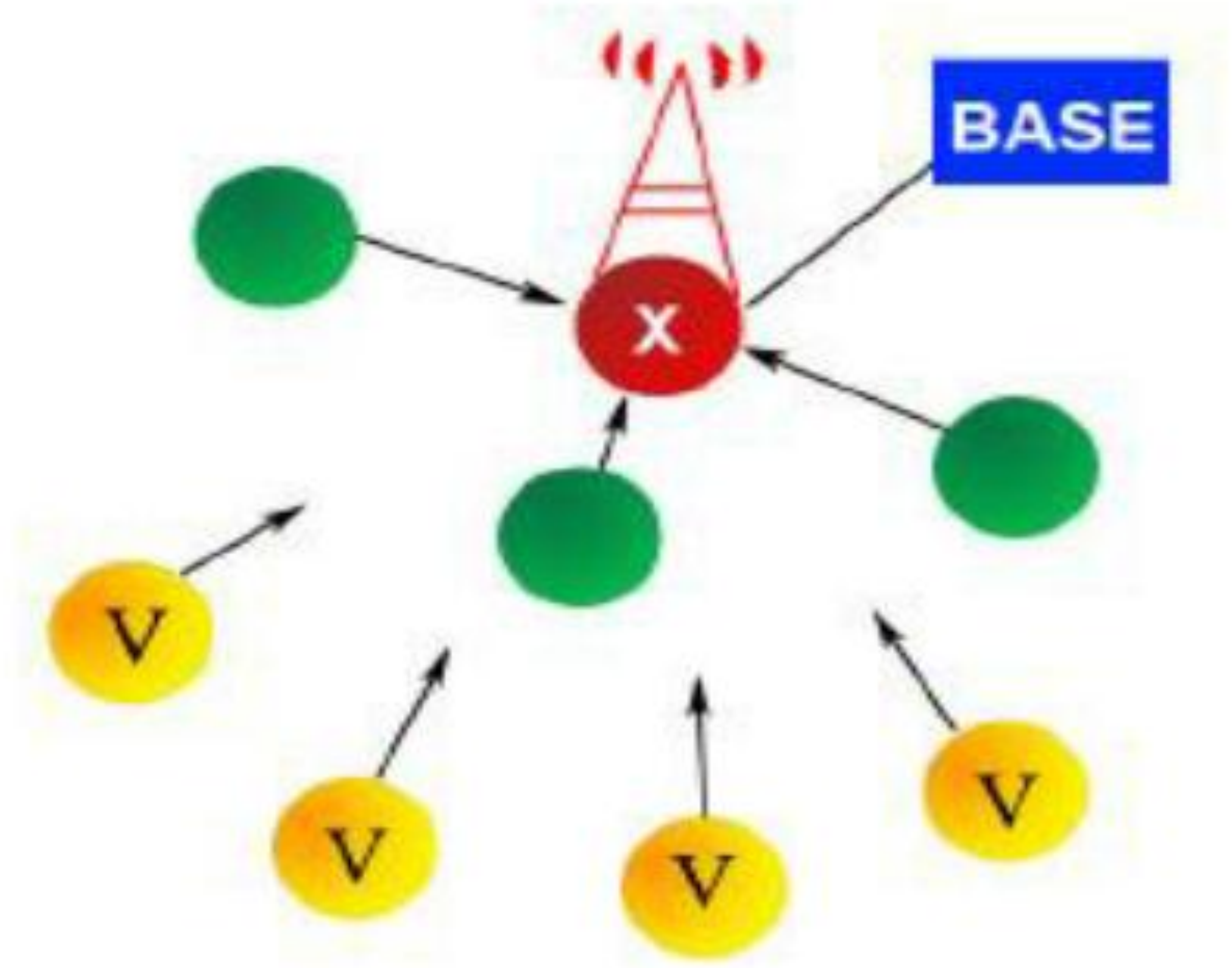
The Sybil attack



WORMHOLE ATTACK



A flood attack (HELLO flood attack)



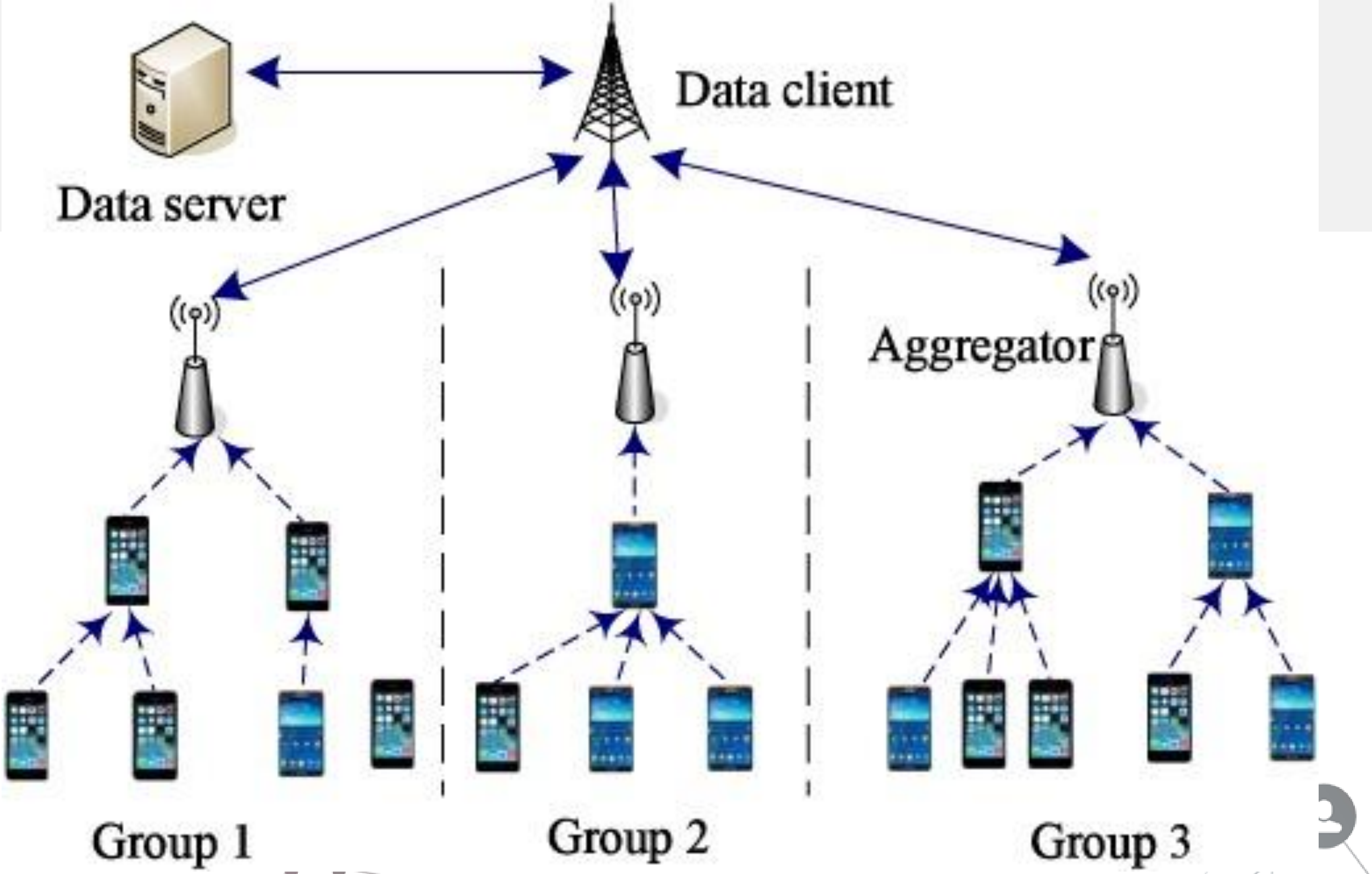
Attacks at the transport level are:

An avalanche attack

Attacks at the transport level are:

The desynchronization attack

Attacks on data aggregation



Recommendations for counteracting attacks on components of the IoT system

Discussions

The list of attacks is an open classification group that can be supplemented and expanded. The implementation of IoT clusters in combination with edge computing requires further research. They need to develop a cluster model and mathematical software for IoT systems in combination with edge computing to minimize information processing and decision-making time.

Conclusions

The analysis allowed us to generalize cyber threats to the components of IoT systems. As a result, it is determined that the largest number of attacks occur on network nodes, and the use of wireless communication technologies between the elements of the system creates the preconditions for a cyber-attack on the system. It is determined that today multi-stage complex protection systems are being implemented, based on the use of the latest technical means, qualified personnel, control procedures, administrative regulations with their strict observance. The analysis of attacks allowed determining their list and exploring the features of implementation. As a result of the analysis and generalization, recommendations for counteracting attacks on the components of the IoT system have been developed.

THANK YOU FOR YOUR ATTENTION!