Advanced IoT Solution for Smart City Eco-monitoring System

Sergey Bezzateev, Natalia Voloshina, Konstantin Zhidanov

bsv@aanet.ru, natali@vu.spb.ru, konstantin.zhidanov@gmail.com

Saint-Petersburg University of Aerospace Instrumentation

Russia

FRUCT 19
7-11 November, 2016
Jyvaskyla, Finland

Outline

- Introduction and previous known solutions.
- Security and scalability for eco-monitoring sensor networks.
- "Galouis" platform.
- Experimental results.

Eco-monitoring on IoT approach

Cities eco-monitoring:

- Structural health: monitoring of vibrations and material conditions in buildings, bridges and historical monuments,
- *Noise urban maps*: sound monitoring in bar areas and centric zones in real time,
- Smart lightning: intelligent and weather adaptive lighting in street lights,
- *Waste management*: detection of rubbish levels in containers to optimize the trash collection routes,

Environment eco-monitoring:

- Forest fire detection: monitoring of combustion gases and preemptive fire conditions to define alert zones,
- *Air pollution:* control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms,
- Landslide and avalanche prevention: monitoring of soil moisture, vibrations and earth density to detect dangerous patterns in land conditions,
- Earthquake early detection: distributed control in specific places of tremors,

Security and emergencies:

- Perimeter access control: access control to restricted areas and detection of people in non-authorized areas.
- Liquid presence: liquid detection in data centres, warehouses and sensitive building grounds to prevent break downs and corrosion,
- *Radiation levels:* distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts,
- *Explosive and hazardous gases:* detection of gas levels and leakages in industrial environments, surroundings of chemical factories and inside mines,

Industrial control:

- Indoor air quality: monitoring of toxic gas and oxygen levels inside chemical plants to ensure workers and goods safety,
- *Temperature monitoring:* control of temperature inside industrial and medical fridges with sensitive merchandiser,
- Ozone presence: monitoring of ozone levels during the drying meat process in food factories,
- Indoor location: asset indoor location by using active (ZigBee, UWB) and passive tags (RFID/NFC).

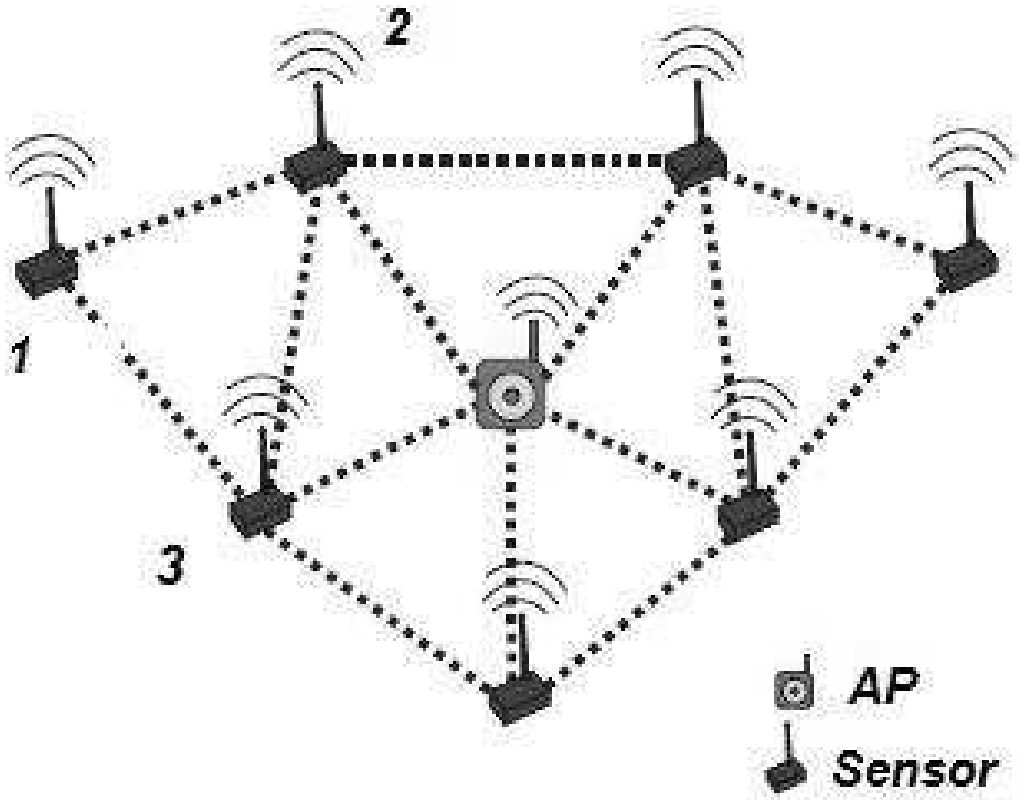
Animal farming:

- Offspring care: control of growing conditions of the offspring in animal farms to ensure its survival and health,
- Animal tracking: location and identification of animals grazing in open pastures or location in big stables,
- *Toxic gas levels:* study of ventilation and air quality in farms and detection of harmful gases from excrements.

Security and scalability for eco-monitoring sensor networks

Two types of devices:

- Gateway or access point(AP) that is used for collecting sensor data.
- Sensors are network devices that are equipped with eco-sensors to collect specified environmental parameters.



Main steps of flexible sensor network creation

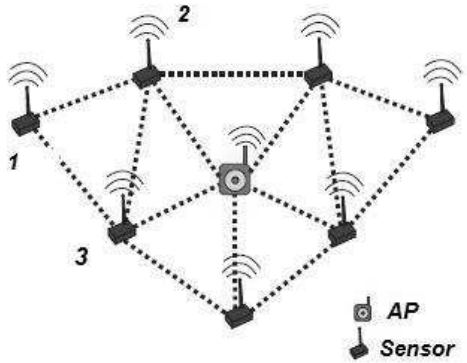
1. **Sensor initialization.** It means that new sensor should be connected to any available sensor from the network or access point (network devices). Two possible scenarios in general:
   - First initialization of several sensors (simultaneously) in one secure network.
   - Adding new sensor to the existing secure sensor network.
2. **Stable sensor network functioning.**
3. **Removal sensor from the sensor network.** In this case there could be two situations:
   - Removed sensor is excluded from particular secure sensor network and could be used in the future only after new network initialization.
   - Removed sensor will be added to another segment of existing secure sensor network.

Master key in security protocol

1. Master key is kept in the so called "tamper resistance memory" of network device (sensor)
   E. Unsal1, M. Milli, Y. Cebi, "Low cost wireless sensor networks for environment monitoring", *The Online Journal of Science and Technology*, v. 6, i.2, 2016, p.61-67
2. Master key is destroyed after predefined time interval.
   J. Jang, T. Kwon and J. Song, "A Time-Based Key Management Protocol for Wireless Sensor Networks", *Proceedings of ISPEC*, 2007, LNCS 4464, pp. 314328.

Obviously for the smart city eco-monitoring purposes the second protocol should be preferred from the point of view to get reliable information about ecological situation in different parts of the city.

First initialization of several sensors for new secure sensor network



- Master key MK is defined for new secure sensor network. Each of sensors i that should be installed should have its own unique identification number ID_i ($ID_i > ID_j$ for $i > j$).
- Sensors exchange their unique identification numbers.
- Each sensor use information about unique identification numbers of other sensors and master key MK to calculate pair-wise keys for mutual authentication. For example, sensor 1 calculates pair-wise keys for sensors $2, 3$:

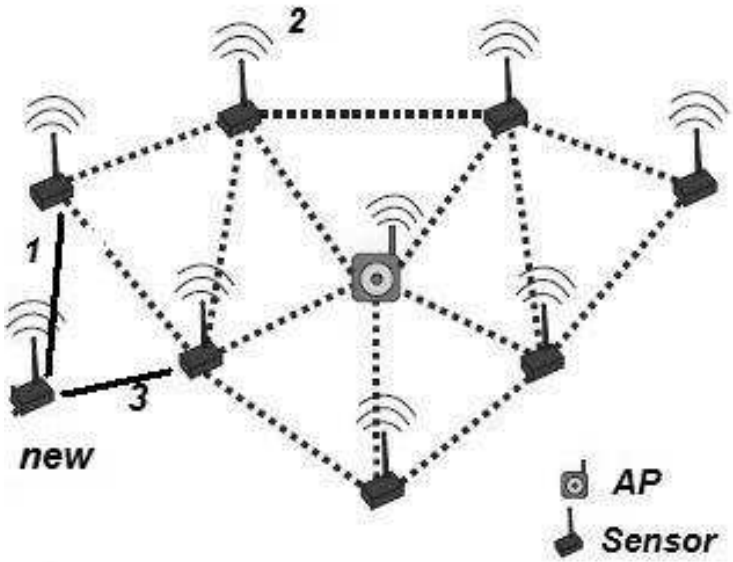
$$K_{1,2} = H(ID_1||ID_2||MK),$$
$$K_{1,3} = H(ID_1||ID_3||MK),$$

- To obtain the scalability feature for this secure sensor network each sensor also calculates auxiliary key $K_{i,i} = H(ID_1||MK)$
- Each sensor deletes its master key MK after predefined time T_{kill}

Stable sensor network

Sensors use pair-wise keys.
For example, sensors 1 and 2 use pair-wise keys $K_{1,2}$ and $K_{2,1}$ consequently.

Adding new sensor to existing secure sensor network



$$K_{new,1} = H(ID_1||MK) = K_{1,1}$$

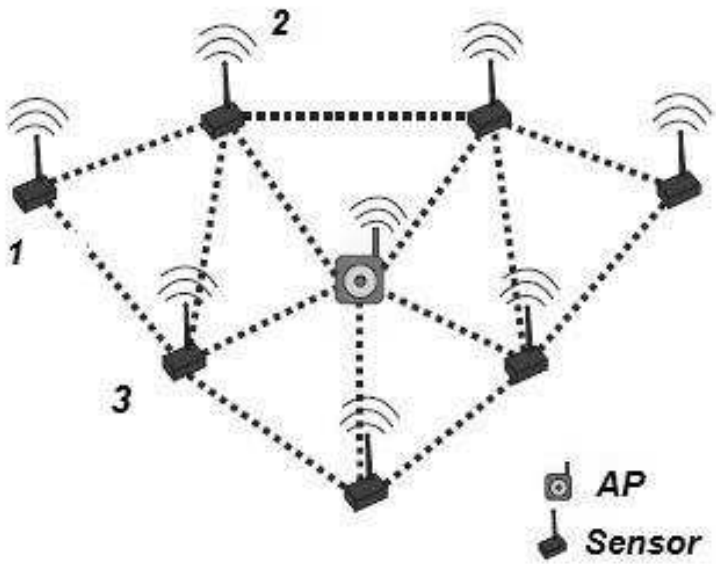
and

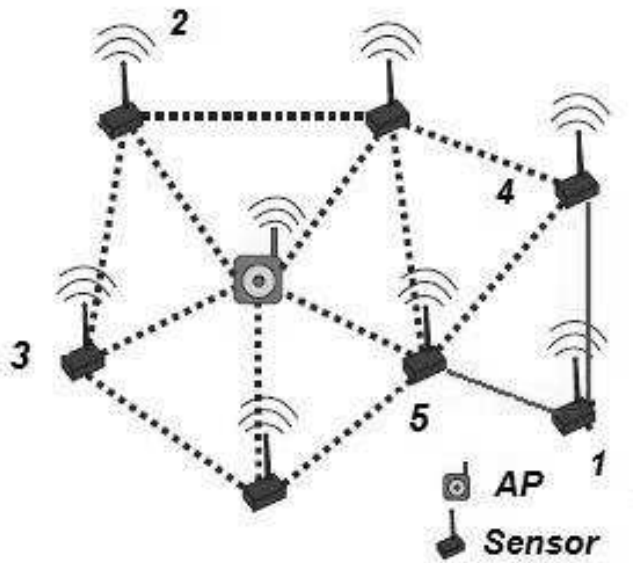
$$K_{new,3} = H(ID_3||MK) = K_{3,3}$$

Before deletion of master key a special key $K_{new,new}$ should be created by new device. As a result new added sensor will store following key sequence $\{K_{new,new}, K_{new,1}, K_{new,3}\}$

Illegal sensor moving to another secure sensor network segment of existing network

In case of illegal movement of sensor from initial secure sensor network segment to the new one without rewriting of its master key MK the process of authentication will be failed.





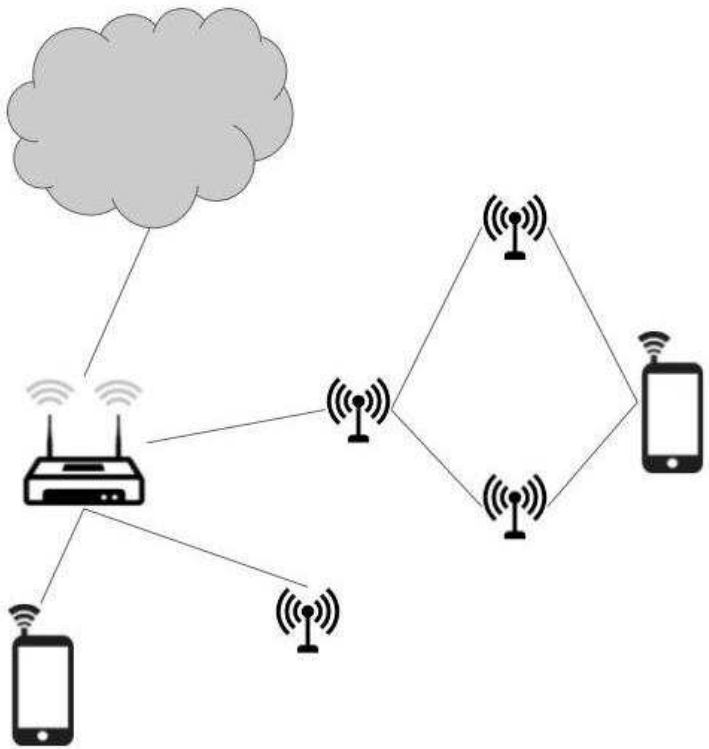


Figure: General scheme for platform "Galouis" using

- Firmware (binary image for ESP8266 chip),
- Android software (Java libraries and sample applications),
- Web software (JavaScript library and sample pages),
- Server-side services (user interface, data processing scripts, DB access scripts),
- Database (MySQL schema).

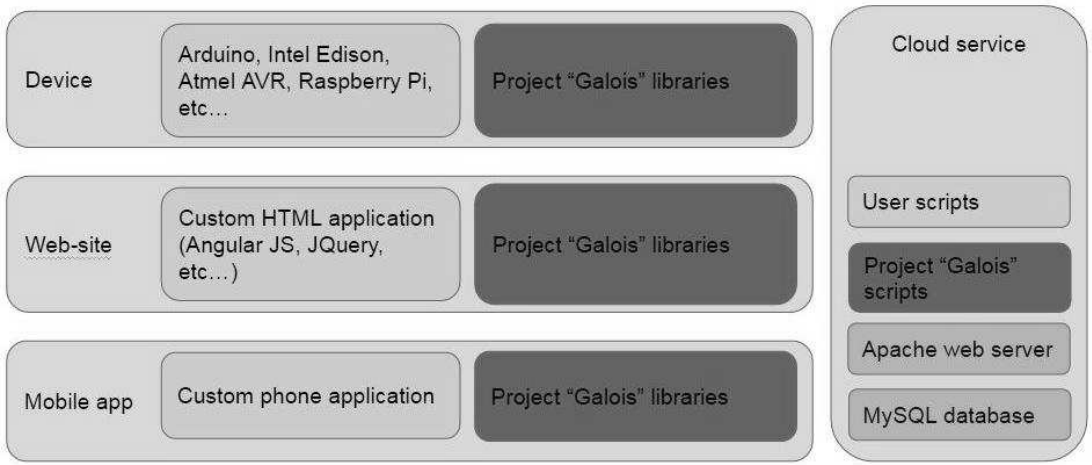


Figure: Components of platform "Galouis"

"Galouis" platform is transparent for developers:

- "duckling" devices by using any possible channel of user Smartphone (Bluetooth, WiFi, IF, or NFC). For example for NFC it is possible to use OPACITY protocol as a part of "duckling" procedure.
  V. Petrov, S.Bezzateev, V. Zybin, "Wireless authentication using OPACITY protocol", *InUltra Modern Telecommunications and Control Systems and Workshops (ICUMT), 7th International Congress*, 2015, Oct. 6, pp. 253-258
- access sharing,
- traffic routing between devices,
- web access to devices,
- setting up WiFi credentials at devices.

Nodes of eco-monitoring network

Prototype of secure eco-monitoring smart city system based on microcontroller $ESP8266$.

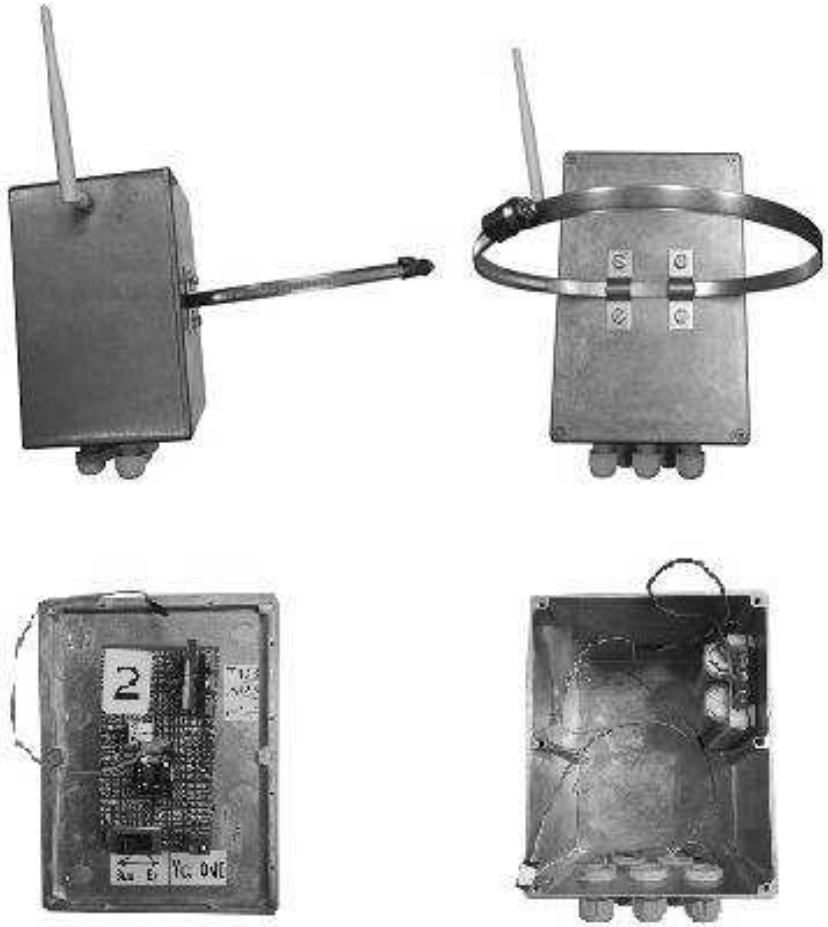


Figure: Sensor box

Eco-sensors

Developed sensors are equipped by eco-sensors of three type: CO_2, radiation and noise level.

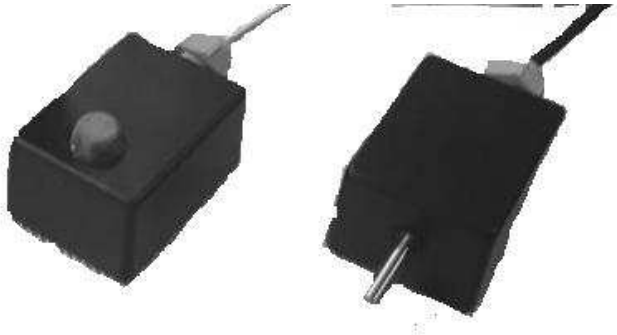


Figure: Data sensors

The prototype of developed secure eco-monitoring IoT system was successfully approved in Saint-Petersburg and Novosibirsk cities in current eco-monitoring Smart City programs.

Conclusion

The possibility of eco-monitoring network-based system with self-organizing sensors constructing is considered. Using a mutual authentication secure protocol together with the "Galouis" platform helps to build an efficient, safe and easily scalable sensor network to collect and process ecological information.

Figure: Kolcovo city

Acknowledgment

This work was partially financially supported by Dell-EMC corporation.

THANK
YOU
FOR
YOUR
ATTENTION !