UDC 621.391

FOG-NETWORK WITH SMART CONTROL SYSTEM MODEL DEVELOPMENT

Piavchyk M., Budishevskyi O., Osypchuk S.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: serg.osypchuk@gmail.com

РОЗРОБКА МОДЕЛІ FOG-МЕРЕЖІ З ІНТЕЛЕКТУАЛІЗОВАНОЮ СИСТЕМОЮ УПРАВЛІННЯ

В даній роботі **запропонована архітектура** мережі **FOG** з інтелектуальною системою управління (**ІСУ**). Акцентовано, що забезпечення технологій **IoT** обумовлює **зростання** об'єму **трафіку** та його **флуктуацій**, в той час як цей трафік повинен бути оброблений з **мінімальними затримками** з метою **прийняття правильних рішень** на основі вмісту IoT-трафіку, що виконує **ІСУ.**

In this paper the **FOG network architecture** with smart control system (**SCS**) is proposed. It is emphasized that the provision of **IoT** technologies causes traffic **increase** and **fluctuations**, while this traffic must be processed with **minimal delays** in order to **make the right decisions** based on the IoT traffic content. Decision making is performed by **SCS**.

Introduction. The paper considers one of the world trends in the modern infocommunication technologies development – ***FOG*** network [1]. In this work, the FOG network is a tool to ensure functioning of another technological trend – Internet of Things (***IoT***) [2].

Since the development of big data and computing networks, several distributed computing paradigms have emerged: ***Clouds***, ***FOG***, and ***Edge***. The ***FOG*** paradigm takes the position *in the middle between* Cloud and Edge; while being as close as possible to *Edge* devices, and FOG partially has the same properties of data storage and computing properties as *Cloud* has. Collecting data from IoT devices and processing those data in FOG network allow *preventing* certain situation, *managing* it, or *regulating* its consequences as quickly as possible.

FOG is defined as a *decentralized* computing infrastructure in which *data*, *computing units*, and *applications* take place *between cloud* and *data sources*, and the resources of such network are used to *store* and *process* data, with access to data locally and over the Internet. FOGs are characterized by proximity to end users, pooling local resources, reduction of delays and capacity savings of the backbone network.

Limited network, storage and computing *resources* necessitate the creation of an efficient and optimal system for managing such resources – *smart control system* (***SCS***), which will manage requests and data from IoT devices by *expanding* or *reducing* network resources, or *keeping* the current amount of computing resources required to process incoming traffic.

Model description. This paper proposes a *model of FOG network*, which involves transporting data from IoT sensors to FOG network and to SCS, processing information in SCS**,** and making decisions in SCS on the impact on *FOG network resources* and the on the *control object* (***CO***) (Fig. 1).

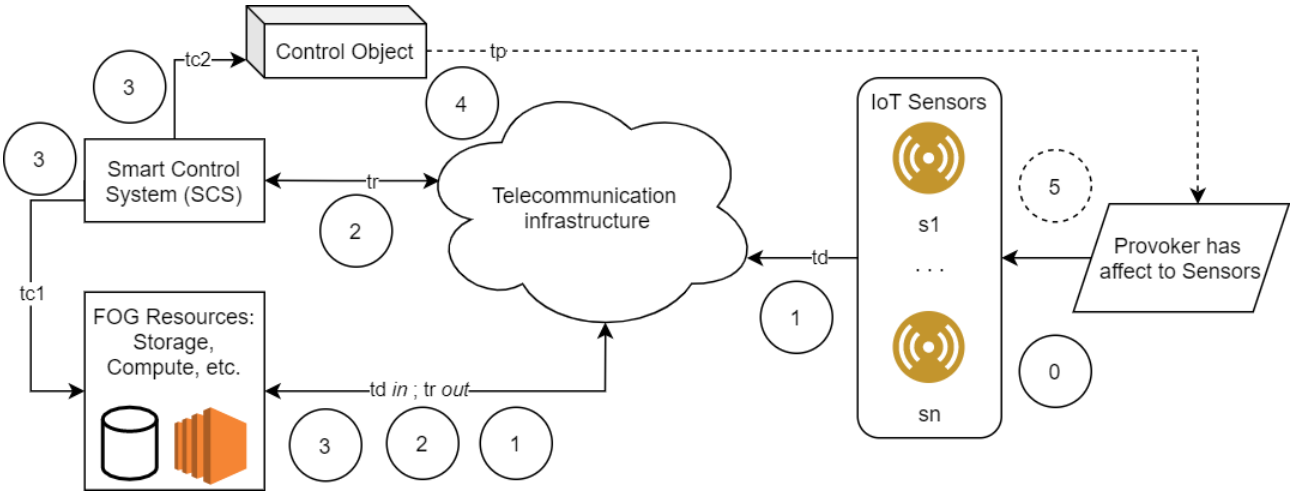

Fig. 1. The FOG network scheme with a smart control system (SCS).

Let us review the proposed FOG network model functionality step-by-step.

Step 0. Suppose there is a specific pathogen that affects IoT sensors.

Step 1. Incoming traffic from sensors s***1***,…, s***n***, with some specified characteristics and parameters:

- number of sensors: ***n,***
- sampling the time of sending data from one sensor: t***d,***
- amount of data sent from one sensor: V***d.***

TC Infrastructure (***TCI***) provides communication between sensors and FOG resources, SCS, CO.

V***s*** data from IoT sensors is written to the *storage resources* of the FOG network for further retention and processing.

Storage resources of FOG network have a certain limited total capacity ***S***, bytes.

Step 2. SCS analyzes the collected information V***s*** at intervals t***r***. SCS attracts or releases the computing resources of the FOG network to provide a necessary computational capacity for analyzing the received data from sensors.

It is important to note that the *computational resources* of the FOG network have a limited performance ***P***, Instructions Per Second (IPS) [3]. The calculations speed in FOG network is influenced by the factor of *calculation complexity* [4]. The *calculations complexity* is influenced by the *incoming traffic type and its characteristics* [5].

Step 3. SCS receives the information from FOG network and makes a decision on the instructions transmission need to the control object CO at discrete intervals: t***c1***, t***c2***. CO can be:

- *Computing resources of the FOG network*, to *attract more* or *release* computing resources for the purpose to process the required amount of data for decision-making by SCS,
- *Other management facilities* that may respond to an event or emergency in an appropriate manner (fire, military, medical, etc.)

Step 4. Response of the CO to the received information at discrete time intervals t***p***. For example, such a response may be the implementation of actions caused by notifying the nearest locations of fire brigades, informing public services about the increased radiation background in the region, responding to an increase in enemy military forces in the region, and so on.

Step 5. As a result of performing actions to respond to the received information, it is expected that in Step 0, but *in subsequent cycles*, the *pathogen may have a modified effect* on IoT sensors, which will lead to *other decisions in the SCS*.

Conclusion. *As shown*, the proposed algorithm for the operation of the FOG network with SCS provides:

- *generating traffic* with certain characteristics *by IoT sensors*,
- *storing and processing data* in the FOG network,
- *SCS implementation* for making decisions on the *FOG-network resource* and *control objects* management, while *enabling learning mechanism* for SCS based on the *IoT traffic flow*, *decisions made,* and *reached effect to control objects*,
- establishing *relationships* between *incoming IoT traffic* and its impact on the *decision* to perform an action or omission on the *control object*.

The next step in this work is to create a *simulation model* according to the proposed scheme of the FOG-network with an *intelligent control system* and discover its behavior when changing the input parameters. The *proposed model* can be used for *different needs of national, local or corporate importance*, in order to effectively respond to changes in the environment.

References

1. FOG networking: [https://en.wikipedia.org/wiki/Fog_computing].
2. Internet of Things: [https://en.wikipedia.org/wiki/Internet_of_things].
3. Instructions per second: [https://en.wikipedia.org/wiki/Instructions_per_second].
4. Computational complexity: [https://en.wikipedia.org/wiki/Computational_complexity].
5. Network traffic: [https://en.wikipedia.org/wiki/Network_traffic].