УДК 004.35:811.111

Korotkevich V., Molchan O.

The Internet of Things

Belarusian National Technical University
Minsk, Belarus

The Internet of Things (IoT) is sensors and actuators embedded in physical objects and linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet [1].

There are three fundamental components that combine to form an IoT node: intelligence, sensing, and wireless communications. The IoT embedded platforms can include sensors like infrared ones, accelerometers and gyroscopes to detect and gather information on real-world objects [2].

Nevertheless there are 2 key challenges:

1) The technology itself. Engineers pushed to leverage the size of micro-electromechanical systems (MEMS) but it seems to be impossible.

2) Most of MEMS comes from smartphones segment. But the IoT world is very different, characterized by a highly fragmented structure of competing technological platforms [3].

There are 3 main options for wireless communication:

1) ZigBee. It is a low-power wireless network that was involved in industrial and building automation. A novel aspect of ZigBee is mesh networking.

2) BLE. A key advantage of BLE is a support of the original Bluetooth, which makes it more robust than ZigBee.

3) Wi-Fi. It is predominant communication technology because it offers the best power-per-bit efficiency. However, power consumption is high [4].

Concerns have been raised that the IoT is being developed rapidly without appropriate consideration of the profound security challenges involved. In fact, there are three major challenges that we cannot ignore: ubiquitous data collection, unexpected uses of data, heightened security risks [4].

Most of the technical security issues are similar to servers, workstations and smartphones, but the firewall, security update and anti-malware systems used for those are generally unsuitable for the much smaller, less capable IoT devices. Without adequate security, intruders can break into IoT systems and networks, accessing potentially sensitive personal information about users, and using vulnerable devices to attack local networks and devices. A significant amount of work has already been done in the EU and USA. There will be stronger regulation for companies developing systems that process personal data to protect security and privacy. Also they can use access control measures and encrypt data.

The IoT and blockchain are two topics which are causing a great deal of hype in the technology circle. The idea that putting them together could result in something even greater than the sum of its parts. For instance, blockchain can be used to track the sensor and prevent duplication with any other malicious data [5]. The other possible applications of the IoT are: healthcare, buildings and utilities.

References:

1. IoT Analytics [Electronic resource]. – Mode of access: https://iot-analytics.com/internet- of-things- definition/. – Date of access: 21.02.2018.

2. IoT [Electronic resource]. – Mode of access: https://www.lanner-america.com/knowledgebase/IoT/. – Date of access: 04.03.2018.

3. Smart Sensors Fulfilling the Promise of the IoT [Electronic resource]. – Mode of access: https://www.sensorsmag.com/components/smart-sensors-fulfilling-promise-iot. – Date of access: 13.03.2018.
4. The fundamental components of the Internet of Things [Electronic resource]. – Mode of access: https://www.electronicsworld.co.uk/news/advertorials/5022-the-fundamental-components-of-the-internet-of-things. – Date of access: 14.03.2018.
5. Blockchain and the Internet of Things: 4 Important Benefits of Combining These Two Mega Trends [Electronic resource]. – Mode of access: https://www.forbes.com/sites/bernardmarr/2018/01/28/blockchain-and-the-internet-of-things-4-important-benefits-of-combining-these-two-mega-trends/#5d90d1d019e7. – Date of access: 16.03.2018.