Internet of Things: Examination of efficiency and safety

Y V Alyshev, O N Maslov, I S Shatalov
Povozhskiy State University of Telecommunications and Informatics, L. Tolstoy str.,
23, Samara, 443010, Russia
E-mail: shatalovivv@gmail.com

Abstract. The paper studies the problem of complex safety in personal area network and local area network in the Internet of Things project's boundaries. The electromagnetic safety analysis of various wireless picocell technologies have realized by statistical simulation with applying the criterion of functional of expected utility. The results of the statistical model are presented. The model’s stochastic variables are «projected economical effect» and «environmental and ergonomic risk»; the determinate variable is internet of things realization cost. Recommendations for the selection of personal area network and local area network elements based on the Bluetooth protocol are given. The model of equivalent radiator for estimation of Internet of Things objects safety is offered. It is shown that the forced switching of all Internet of Things elements to radiation mode is an «energy threat» for sensors in the room.

Keywords: Internet of Things, Personal Area Network, Local Area Network, wireless picocell technologies, safety examination, statistical simulation method, functional of expected utility, environmental and ergonomic risk.

1. Introduction
Picocell (PCS) technologies are the basis for the wireless integration of electronic devices of various types and purposes - radiotelephones, computers, and digital video cameras, including the elements of the Smart House [1-5]. The integration of PCS-technologies with the Internet within the framework of Internet of Things (IoT) conception [6-9] implements a qualitatively new, synergetic stage of their joint development.

IoT infocommunication networks can be divided into four groups:
- Personal Area Networks (PAN) are located in close proximity to both “things” and ordinary “biological” Internet users;
- Local Area Networks (LAN) are located on the territory within one or a small group of buildings (residential building, office, enterprise, company);
- Metropolitan Area Networks (MAN) are combining LANs within the city;
- Wide Area Networks (WAN) are connecting network elements dispersed over distances of the order of $10^3...10^4$ and more kilometres from each other.

The range and versatility of the operation mode of PCS-modules (and also acceptable radiation intensity at low power consumption; resistance to interference; lack of influence on radio-electronic equipment (REE) and other electronics; low cost, etc.) make them indispensable at the PAN level networks. At the LAN level, the most winning option seems to be their use in highly efficient and economical multi-storey building management systems.
The global objectives and goals of the IoT project are discussed in [1-2]. Design methods for sensor networks are described in sufficient detail in [3-4] and [10], as well as in [5], which presents theoretical design principles. Key protocols are described in publications [6-7]; standardization problems are briefly discussed in [8]. A wide range of practical possibilities and prospects for the use of IoT are demonstrated in [9-10], as well as in [11-13].

In the literature issues of ensuring complex IoT security are considered in less detail, a typical example is [14]. Another important drawback is the lack of analysis of the alleged effectiveness of the IoT project; for example, it can be done from the standpoint of both classical theories of expected utility: the von Neumann – Morgenstern objective theory [15] and the Savage subjective theory [16], as well as the theory of prospects and risk [17]. This is largely due to the difficulty of choosing a quantitative criterion for assessing the expected utility of the IoT project by analogy with other applications of the theory of expected utility [18], as well as the corresponding software and experimental data.

Similar problems emerge when developing systems for protecting information from leakage into the external environment through “random antennas”. The effective solution is the computer method of statistical simulation modeling (SSM) [19-21], which combines analytical calculations with probabilistic combinatorics according to the Monte Carlo methods [22-23]. The initial data for simulation can be obtained by experimental and heuristic methods [24].

This work illustrates the application of the SSM method and the functional of expected utility (FEU) for solving the scientific and technological problems: examination of the effectiveness and safety of the IoT project. The proposed method combines the advantages of mathematical modeling and probabilistic combinatorics using data characterizing the economic, environmental-ergonomic, and information security of IoT systems and networks.

2. Composition and structure of FEU

We are using the multi-factor model of FEU. It is formed according to the scheme: “relative gain \( X_k \) plus relative saving of resources \( Y_k \) plus change in risk \( V_k \)” [9] as a criterion for evaluating the effectiveness of a collective project carried out under the conditions of Germeier’s game by \( N \) participants with opposing interests [10]. Let \( K \) be the total number of ”scenarios” (options for implementing the IoT project) available for decision makers; \( k \) \([1; K]\) is the scenario number. Let \( F_k \) denote the general positive effect (gain) predicted by the decision makers with a total cost of resources equal to \( G_k \), which can be provided by them with probability \( P_{G_k} \). The probability values \( P_{F_k} \) and \( P_{R_k} \) take into account, accordingly, the correctness of the prediction of the decision makers to get at the project exit according to the \( k \)-th scenario the gain \( F_k \) and the specified (environmental-ergonomic, economic, informational) risk \( R_k \), and the probability value \( P_{U_k} \) is the chance of the decision maker to obtain permission to carry out the project under this scenario.

A component of the FEU showing savings of resources is represented as

\[
Y_k = P_{Nk} \frac{G_k}{0} \sum_{n=1}^{N} \left( P_{G_{n}} G_{n} + P_{U_{n}} U_{n} \right),
\]

where \( P_{G_{n}} \) is probability of obtaining the resource \( G_{n} \); \( P_{U_{n}} \) is probability of effective project promotion by allocating funds \( U_{n} \) for its advertising for the \( n \)-th project participant, \( n \) \([1; N]\); \( P_{R_{k}} \) is probability of agreement between all \( N \) participants to start a project (note that accounting funds \( U_{n} \) for advertising is in this case an important feature of the project, see below for more details). Similarly, the risk component is

\[
R_k = P_{Mk} R_0 / \sum_{m=1}^{M} R_m ,
\]

where \( R_m \) is the risk for the \( m \)-th object in the framework of the project, which has to be considered by its participants, \( m \) \([1; M]\); \( P_{M_k} \) is probability of the agreement between its participants to hand the completed project for approval, attractiveness (comparative effectiveness) of the project is \( X_k = F_k / F_0 \). Then FEU will have form:

---

IET-2020
IOP Conf. Series: Materials Science and Engineering 873 (2020) 012001 doi:10.1088/1757-899X/873/1/012001
\[
Q_k / Q_0 = P_k \left[ P_F \left( F_k / F_0 \right) + P_N / \sum_{n=1}^{N} \left( P_{Gn} / G_n + P_{Un} / U_n \right) \right] + P_M / \sum_{m=1}^{M} R_m \]
\]

Where \( G_0; F_0; R_0 \) and \( Q_0 \) are the amount of resources, the gain, the risk and the FEU for the base case (with \( k = 0 \)); they are conditionally accepted as the basis for comparison by decision makers (DM). The scheme for determining FEU in the interest of assessing the effectiveness of the IoT project is illustrated by the scheme in Figure 1.

![Figure 1. The algorithm for the formation and selection of the maximum FEU](image)

After aggregation elements (1) FEU becomes to a compact form:
\[
Q_k / Q_0 = P_k \left( P_F X_k + P_Y Y_k + P_R V_k \right)
\]

(2)

The most “understandable”, in fact, deterministic component of (2) is \( Y_k = R_G G_0 / G_k \), since both the cost of resources and the probability of their receipt by the decision makers can be accurately predicted heuristically: by cost estimates for each \( k \)-th version of the project.

This cannot be said about the components \( X_k = F_k / F_0 \) and \( V_k = R_0 / R_k \), since it is impossible to predict the expected incomes and the change in environmental risk in the same way, and the probabilities \( P_F = \exp(-\gamma X_k) \) and \( P_R = \exp(-\beta V_k) \) associated with them according to [8–9] can only be specified with accuracy to parameters \( \beta [\beta_{\text{MIN}}; \beta_{\text{MAX}}]; \gamma [\gamma_{\text{MIN}}; \gamma_{\text{MAX}}] \). These parameters are formalizing the uncertainty of knowledge of various decision-makers about the properties of the random components of FEU: \( X_k [X_{\text{MIN}}; X_{\text{MAX}}] \) and \( V_k [V_{\text{MIN}}; V_{\text{MAX}}] \).

Probability is \( P=1-\exp(-X_k) \) and after calibration \( Q_k = Q_0 =1 \) with \( X_0 = Y_0 = V_0 =1 \), FEU (2) becomes:
\[
Q_k / Q_0 = \left( 1 - \frac{\exp(-\beta) + \exp(-\gamma)}{\exp(-\beta) + \exp(-\gamma) + 1} \right) X_k Y_k V_k \times (X_k \exp(-\gamma X_k) + Y_k \exp(-\beta Y_k))
\]

(3)
In the structure of model (1) - (3), in addition to the determinate component (a possible variable of simulation) \( Y_k \), there are two stochastic variables: \( X_k \) and \( V_k \), as well as two secondary random parameters: \( \beta \) and \( \gamma \). Figure 1 illustrates the algorithm for determining the FEU (2). The initial stages common to all K scenarios are the analysis of the subject area and the choice of the base case. Then, for each k-th option, actions are performed and highlighted by a dashed contour; at the final stage, the largest value of the FEU \( Q_k/Q_0 \) is selected for all options.

We adapt the FEU to the conditions of the problem: we mean \( N \) REE implementing the IoT project as participants; \( G_n \) is amount of resources determined by the costs of the acquisition, installation and operation of the n-th REE; \( U_n \) has the same meaning; \( R_m \) is risk for the m-th Internet user or any other “biological” object, including the decision-maker involved in the IoT project; \( F_k \) is a gain in respect of which so far it can only be said that, according to the forecasts of the decision-maker, it should be multifactorial and radically large [1-2]. The virtual components \( F_k \) and \( R_m \) significantly “exceed” the real components of the FEU \( G_n \) and \( U_n \) due the uncertainty of knowledge, which can be accurately estimated using the functional-cost analysis.

What are the gain, resources and risk in (1) - (3)? It depends on the subject area and models of objects in the k-th project. The FEU model helps to understand that promotion of the project to the level of profitability is impossible without active (targeted, creative, etc.) advertising in the media, which should include social networks. This is an objective necessity in "digital" economy, where the investment of resources in equipment \( \sum_{n=1}^{N} G_n \) should be supplemented with funds \( \sum_{n=1}^{N} U_n \) for intensive advertising of the project, since without it, it’s no possible to receive a “bonus” in the form of \( F_k \) from consumers, according to (1).

Therefore, the FEU criterion becomes almost the only objective, true and convincing indicator of the effectiveness of the IoT project. The strategic plan of interested decision makers becomes obvious: “invest” in the FEU’s component: \( \sum_{n=1}^{N} U_n \) and get the consumer to pay for it and for \( \sum_{n=1}^{N} G_n \), by intensive formation of \( F_k \) as soon as possible. On the way to achieving this goal, all means are good, since it is a matter of survival of the indicated decision-makers, not their ethics or aesthetics. However, the environmental-ergonomic and informational components \( \sum_{m=1}^{M} R_m / R_0 \) are no less important in the composition of FEU (1) - (3) for consumers of the Internet of Things services.

3. Initial data for simulation

We will consider the features of PCS-technologies using the example of Bluetooth, designed to transmit data over distances of up to 10m (with possibility of increasing range up to 100m), which allows you to connect telephones, computers, and other peripheral devices to the network without providing direct visibility between them. Note that the development of Bluetooth in 1994 by Ericsson Mobile Telecommunication began with a relatively modest goal: to obtain an economical and cheap interface for communication between a cell phone and a headset. However, then the creators of Bluetooth decided to do the same with computers, air conditioners, video cameras, coffee makers, refrigerators and vacuum cleaners, which are directly related to the concept of “Internet of Things”.

It’s important for IoT, that the Bluetooth protocol supports both point-to-point and point-to-multipoint connections. Using the common channel REE form a PicoNet, in which one of them works as the main (Master), the others work as subordinates (Slave). The piconet can have several active subordinate REEs, while the rest are in standby mode, remaining are synchronized with the main ones. Interacting piconets form a distributed network (Scatter Net). It is believed that Bluetooth continues to distinguish itself from other PCS technologies by its versatility and close to the optimal ratio between price and functionality [5]. The most important parameter of the REEs for security examination of PCS technologies within the framework of the IoT concept is the transmitter power \( P_t \), mW.

By \( P_t \) level, Bluetooth devices are divided into three power classes (PC):
- PC-1: maximum power 100 mW, range up to 100 m;
- PC-2: maximum power 2.5 mW, range up to 10 m;
- PC-3: maximum power 1 mW, range up to 0.1 m;

In Russia, the use of Bluetooth REEs at frequencies of 2400 ... 2483.5 MHz was allowed in 2003 for PC-1 and PC-2, and the PC-1 is the most popular. Examples of other wireless technologies for IoT on the market are shown below [2]:
- ML-Node-Z sensor nodes (they are manufactured by Mesh Logic, Russia), IEEE 802.15.4 standard;
- Zig Bit sensor nodes (Atmel, USA), IEEE 802.15.4 standard;
- Z-Wave modules (ITU ITU G.9959 specification);
- Zig Bee sensors (Zig Bee international alliance), IEEE Std 802.15.4 standard;
- BLE (Bluetooth Low Energy), an energy-efficient development of the Bluetooth Special Interest Group.

The maximum and minimum values $P_k$ of the transmitters of listed devices are shown in Table 1; it can be seen that all these REEs are related to PC-3. A comprehensive security review of the IoT project (even by the SSM method) is the serious challenge. However, the examination of REEs’ EMR seems to be an exception, since here one can use the mathematical apparatus of radio engineering systems and the traditional theory of probability [5].

### Table 1. Transmitter power of IoT REE

| Type            | $P_{\text{AMIN}, \mu W}$ | $P_{\text{AMAX}, \text{mW}}$ |
|-----------------|---------------------------|-------------------------------|
| ML-Node-Z       | 4                         | 1                             |
| Zig Bit         | 1.6                       | 2                             |
| Z-Wave          | 10                        | 1                             |
| BLE             | 10                        | 1                             |
| Zig Bee         | 0.6                       | 1                             |

4. Risk simulation results

Let us consider the methodology and conditions for the SSM experiment of the project "Smart House" in the form of a three-room apartment of 100 m², the room is equipped with $N \geq 80$ REEs Bluetooth PC-1 ... PC-2. Six PCS network operating modes were simulated:
- mode No. 1: "constant" radiation, $N >> 1$, Bluetooth PC-2;
- mode No. 2: "alternating" radiation, $N >> 1$, PC-2 Bluetooth; we need to take into account their separation into four groups according to the values of $k$, depending on the schedule of daily activity;
- mode No. 3: "constant" radiation, $N/2 >> 1$, PC-2 Bluetooth and $N/2 >> 1$, PC-1 Bluetooth;
- mode No. 4: "alternating" radiation, $N/2 >> 1$, PC-2 Bluetooth and $N/2 >> 1$, PC-1 Bluetooth; we need to take into account their separation into four groups similar to mode 2;
- mode No. 5: "constant" radiation, $N >> 1$, PC-1 Bluetooth (which corresponds to the "energy threat" in our terminology);
- mode No. 6: "alternating" radiation, $N >> 1$, PC-1 Bluetooth, it is similar to mode No. 2.

The SSM program of the situation in the room where the IoT network is deployed provides for M-fold "playing" using the Monte Carlo method of the values $V_n [0; 1]$ and $r_n [0.3; 10]$; these values are accepted equally probable within the specified limits in accordance with the "principle of indifference".

Next, we calculate the S-fold total level of energy flux density $EFD = \sum_{i=1}^{4} k_i \sum_{n=1}^{N} EFD_{ni}$ for $N = 50...500$; $M = 10^3...10^4$ and $S = 10^3...10^4$. According to the results of statistical processing of data arrays obtained with data level $S$, estimates of the predicted average value of the $EFD_{\text{avg}}$ are determined, as well as the boundaries of the $EFD_{0.05}$ and $EFD_{0.95}$ of the confidence interval corresponding to a probability of 0.90. Table 2 presents the indicated estimates of $EFD$ depending on the number of REEs $N$ involved in the IoT project as an example. Unsafe $EFD$ levels are shown in bold [6].
Table 2. Values of EFD$_{avg}$, EFD$_{MAX}$; boundaries of the confidence interval of the EFD; μW / cm$^2$ for mode No. 5 of REE PC-1

| N   | 50  | 100 | 200 | 300 | 400 | 500 |
|-----|-----|-----|-----|-----|-----|-----|
| EFD$_{0.05}$ | 0.1 | 0.2 | 2.0 | 5.2 | 8.0 | 11.0 |
| EFD$_{avg}$   | 1.6 | 3.2 | 6.7 | 11.3| 16.4| 19.0 |
| EFD$_{0.95}$  | 5.0 | 7.2 | 13.5| 19.0| 27.0| 28.0 |

The recommended way to “improve” the indoor environment is to switch to using PC-3 REEs, since all EFD levels (as shown in table 2) are reduced by two orders of magnitude and the value of EFD is <6 μW / cm$^2$ even at N = 500. The aforesaid is confirmed by the data in Table 3 for mode No. 2 when using PC-3 REEs; it is clear that the situation with electromagnetic radiation in this case is safe, and the “energy threat” is impossible in principle.

Table 3. Values of EFD$_{avg}$, EFD$_{MAX}$; boundaries of the confidence interval of the EFD; μW / cm$^2$ for mode No. 2 of REE PC-3

| N   | 50  | 100 | 200 | 300 | 400 | 500 |
|-----|-----|-----|-----|-----|-----|-----|
| EFD$_{0.05}$ | 0.001| 0.008| 0.030| 0.044| 0.068| 0.084|
| EFD$_{avg}$   | 0.013| 0.031| 0.058| 0.082| 0.107| 0.139|
| EFD$_{0.95}$  | 0.040| 0.076| 0.110| 0.144| 0.160| 0.204|

5. Statistical simulation of FEU

Variables and random parameters (3) are played by the Monte Carlo method according to a uniform distribution within the limits determined by decision makers by an expert method; thus, each combination of the indicated parameters and variables corresponds to one FEU value, and after $N_p$-fold repetition of this procedure, array of $N_p > 1$ FEU values is formed. This array is subjected to standard statistical processing:

- the histogram is built within $(Q_k / G_0)_{MAX}$; $(Q_k / G_0)_{MIN}$ for $N_c$ intervals found by the Sturges formula;
- the expected value (average value), the variance and the boundaries of the 90% confidence interval are determined: $(Q_k / G_0)_{0.95} \text{ and } (Q_k / G_0)_{0.05}$.

Figure 2. Histogram of $Q_k / Q_0$

In addition to the initial data, the histogram of FEU and its parameters all $N_p = 10^3$ played values of the FEU are displayed, which can be viewed. Analysis of specific options shows that when the number of similar REEs is reduced to N = 100, resource savings are $Y_k = 5$, risk change is $V_k [1; 5]$, attractiveness reduction of the project is $X_k [0.2; 1]$ and the uncertainty of the knowledge of decision makers about
development of the situation is corresponded to $\beta [0;0.1]; \gamma [0; 0.1]$. According to the data in Figure 2, this leads to a noticeable improvement in all the characteristics of FEU despite the negative dynamics of $X_k$.

Similarly, if replace PC-1 with PC-3 with a five-fold increase in the number of REEs result in $Y_k = 2.5; V_k [1; 2.5]$ and $X_k [0.5; 1]$, then this is also be justified from the point of view of the growth of the parameters of the FEU. In both cases the cause can be considered the prevalence of the resource saving factor $Y_k$ in the structure of the FEU with a relatively stable $V_k$ and an acceptable decrease in $X_k$.

6. Discussion
The decision-maker can use a computer to get answers to all questions of interest by forming the initial data using any available information about the project. A broad field of activity for virtual research of the effectiveness of various options for implementing the IoT project opens up for the decision maker, since the considered fragment of the SSM model is the open system and it operates in a dialogue mode. The ability to select the initial values of parameters $\beta$ and $\gamma$, which evaluate the most uncertain factor of knowledge uncertainty for analysis, allows decision makers to set them close to zero, and then vary within the necessary limits, checking the response of the FEU to their dynamics. It should be remembered that the SSM model is a “device” in the hands of the decision maker, which performs a significant part of the work for it, but it is not able to completely replace him.

7. Conclusion
A comprehensive examination of the Internet of Things project is possible using the SSM method, which is combining the methods and means of mathematical modeling with probabilistic combinatorics and the FEU criterion. It is necessary to pay attention to both informational [3-4] and environmental-ergonomic safety based on the EMR factor of wireless PCS technologies, on the basis of which PAN and LAN are built when implementing the project [5-6]. The preferred elements of IoT networks based on the Bluetooth protocol are PC-3, on condition that a rational way of deploying radio electronic equipment will compensate the negative consequences of increasing their number compared to more powerful PC-1s’.

References
[1] Overview of the Internet of things 2012 (ITU-T Rec) Y.2060.
[2] Architecting the Internet of Things 2011 (Springer) 351 p.
[3] ISO/IES JTS 1. Technical Document of ISO/IES 1 Study Group on Sensor Networks (SGSN). Version 3 2009 166 p.
[4] Sensor networks and configuration: fundamentals, standards, platforms and applications 2007 (Springer) 510 p.
[5] Dargie W, Poelabauer C 2010 Fundamentals of Wireless Sensor Networks Theory and Practice (John Wiley & Sons Ltd) 311 p.
[6] Hersent O, Boswarthick D, Elloumi O 2012 The Internet of Things: Key Application and Protocols (Willey) 370 p.
[7] Cook D, Das D 2005 Smart Environments. Technologies, protocols and applications (Hoboken NY: Wiley-Interscience) 404 p.
[8] Atzori l, Iera A, Morabito G 2010 The Internet of Things: A survey (Computer Networks) 54 pp 2787-2805.
[9] Bandyopadhyay D, Sen J 2011 Internet of Things: Application and Challenges in Technology and Standardization (Wireless Personal Communications) 58 (1) pp 49-69.
[10] Kuniavsky M 2010 Smart Things: Ubiquitous Computing User Experience Design (Morgan Kaufmann) 336 p.
[11] McEwen A, Cassimally H 2013 Designing the Internet of Things (John Wiley & Sons) 260 p.
[12] Vasseur J, Dunkels A 2010 Interconnecting smart objects with IP (Morgan Kaufmann) 432 p.
[13] Zhou H 2012 The Internet of Things in the Cloud:A Middleware Perspective (CRS Press) 365 p.
[14] Evdokimov S, Fabian B and Günther O 2011 *RFID and the Internet of Things: Technology, Application and Security Challenges* (Now Publishers Inc) 88 p.

[15] Von Neumann J and Morgenstern O 2004 *Theory of Games and Economic Behavior: Second Edition* (Princeton: Princeton University Press) 625 p.

[16] Savage L J 1954 *The Foundations of Statistics* (N.Y.: Wiley) 310 p.

[17] Kahneman D and Tversky A 1979 *Prospect Theory: An Analysis of Decision under Risk* (Econometrica XVI) pp 263-291.

[18] Shoemaker Paul J H 1982 *The Expected Utility Model: Its Variants, Purposes, Evidence and Limitations* (Journal of Economic Literature) XX(2) pp 529-563.

[19] Maslov O N, Rakov A S and Silkin A A 2013 *Statistical Simulation of Random Antennas like Development of the Statistical Theory Antennas* (Proceedings of the IX International Conference on Antenna Theory and Techniques ICATT’13 – IEEE Ukraine, September 16-20 Odessa) pp 53-58.

[20] Maslov O N, Rakov A S and Silkin A A 2013 *Statistical Characteristics of the Field of an Array of Random Aperture Antennas* (Journal of Communications Technology and Electronics) 58(11) pp 1056-1064.

[21] Maslov O N, Rakov A S and Silkin A A 2015 *Statistical Models of the Wave Field of a Random Aperture Antenna* (Journal of Communications Technology and Electronics) 60(6) pp 603-610.

[22] Maslov O N and Shatalov I S 2018 *The Simulation of Equivalent Currents Exciting a Stochastic Aperture Radiator* (Proceedings of SPIE Vol. 10774) pp. 107740S-1 – 107740S-9 doi: 10.1117/12.2317729

[23] Maslov O N and Shatalov I S 2019 *Simulation of Statistical Characteristics of Aperture Random Antenna by Triad-Cluster Method* (Proceedings of SPIE Vol.11146) pp 11146A-1–11146A-13 doi: 10.1117/12.2524835.

[24] Maslov O N 2018 *Electromagnetic Safety of Workstations Equipped with Active Systems for Data Protection* (Journal of Communications Technology and Electronics) 63(2) pp 163-172.