The 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
21-23 September, 2017, Bucharest, Romania

Modelling of Healthcare IoT Using the Queueing Theory

Anastasiia Strielkina, Dmytro Uzun, Vyacheslav Kharchenko
Department of Computer Systems and Networks of National Aerospace University "KhAI", Kharkiv, Ukraine,
a.strielkina@csn.khai.edu, d.uzun@csn.khai.edu, v.kharchenko@csn.khai.edu

***Abstract*—In the field of health, networked medical devices are closely intertwined in the structure of the Internet of things.**

A healthcare IoT infrastructure with a brief description of each component is presented. These components are a device with a reader, Cloud, healthcare provider and communication channel. As the title implies the paper presents simple cases with a few models of healthcare IoT system based on the queueing theory. The models describe streams of the requests and attacks on vulnerabilities and procedure of recovery by restart and eliminating of ones.

Keywords—Cloud; healthcare; insulin pump; Internet of Things; Markov process; queueing theory; vulnerability; security

I. INTRODUCTION

The Internet of Things (IoT) is a new step in technological progress. The IoT allows people and "things" to connect anytime, anywhere using a variety of communication networks. According to the preliminary forecasts [1-2], about 50 billion devices will be connected to the Internet and the IoT market will reach about $1.7 trillion by 2020.

The Internet of Things represents new, exciting opportunities for almost every area of our life. And, of course, a healthcare is not an exception. The IoT can significantly improve the existing healthcare system.

Modern medicine has risen to an unattainable level earlier over the past decade. Today, the healthcare sector is a high-tech industry, where all areas of medicine are successfully developing that can save lives of previously hopeless patients. The technical equipment of medical institutions has significantly improved, it has become possible to diagnose the disease at the earliest stage and to quickly restore the working capacity of patients.

According to the forecasts of the researchers [3], the market of medical IoT gadgets and IoT-applications will grow to $136.8 billion in 2021.

The IoT in healthcare provides opportunities:

- To obtain, analyse and share patient health data.
- For personalized treatment that can be given at a more detailed level.
- For interaction between individual devices with the entire healthcare system, etc.

~~The Internet of things will allow to monitor patients, track their location and condition (control of temperature, pressure and other physical indicators), as well as monitor the medical institution itself, its internal microclimate.~~

One of the most widely used IoT devices is an insulin pump. According to the statistics ~~of the World Healthcare Organization~~ [4], about 8.5% of the world population had diabetes in 2014. ~~The diabetes epidemic has serious health and socio-economic consequences.~~ This confirms the relevance of the applicability of such devices. The insulin pump can be placed in an inconspicuous place under the clothes, so a patient can carry out and control the injection of insulin with a special console or smartphone.

In this paper, authors presented a simple model using the queueing theory of the ~~healthcare~~healthcare IoT system. There are many solutions that allows using smart sensors working with clouds, different types of devices. In this case, it is proposed to develop a complex system that allows taking into account the specificity of end user devices, communication channels, technologies of data flows. With all the variety of existing techniques, mathematical models of such solutions are extremely rare in the literature.

The remainder of the article is structured as follows. Section 2 presents a healthcare IoT infrastructure with a brief description of each component. Section 3 presents a justification of applicability possibilities of the queueing theory and presents a case study for considered system followed by concluding remarks.

II. HEALTHCARE IOT INFRASTRUCTURE

A typical healthcare IoT system consists in general of such components as depicts Fig. 1.

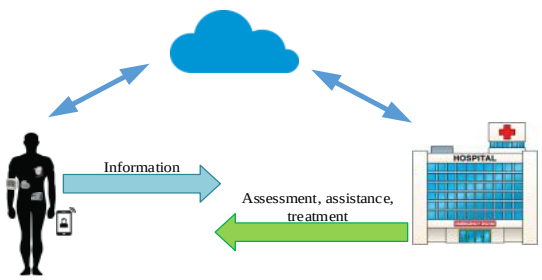

Figure 1. Main components of healthcare IoT infrastructure:

devices with a reader, Cloud and a healthcare organization

Thus, the constituent components of the healthcare IoT infrastructure are: (1) Cloud, (2) device (with a reader, also often called as a "base station"), (3) medical or healthcare providers and (4) communication channels between device and Cloud, and healthcare provider and Cloud (Fig. 2).

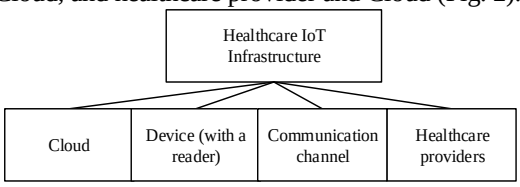

Figure 2. Detailing of components of healthcare IoT infrastructure

The number and variety of devices have increased significantly. According to [5] healthcare and medical devices can be classified as:

- Consumer products for health monitoring.
- Wearable, external medical devices.
- Internally embedded medical devices.
- Stationary medical devices.

Such devices sense electrical, thermal, chemical, and other signals from the user's body. They directly sense and collect biomedical signals, that is, information about the physical and mental state of human's health.

Therefore, FDA provides risk-based classification [6-7] of the considered devices:

- Class I – low risk – general controls (least amount of regulatory control).
- Class II – medium risk – general and special controls (assure safety and effectiveness).
- Class III – high risk – general controls and premarket approval (support or sustain human life).

It is understandable and logical that the insulin pump refers to the Class III because a human's life depends on its performance.

Main limitations of devices are small storage, limited energy and computational capabilities.

For communication with the Cloud, devices frequently use external devices that are referred as the readers (i.e. laptops, smartphones, etc.). Thus, the data can be sent to the Cloud directly or indirectly (through the reader). The reader is less severe because it has own resource constraints.

Many communication technologies are well known and used in the IoT such as WiFi, Bluetooth, ZigBee and 2G/3G/4G cellular.

Inasmuch as devices and readers are resource-constrained, received data from sensors are usually sent to Cloud servers. This data are processing and storage for a long term there. Authorized users (medicine and healthcare providers) have access to this data at any time and in any place.

Healthcare providers include medical and healthcare professionals, organizations and their business associates, insurance companies, etc. As before, the central place in the treatment will be occupied by specialists – doctors and medical personnel. The Internet of things will help them to work more effectively.

Explanation of the functions, activities and interrelationships of the main components is depicted in Fig. 3.

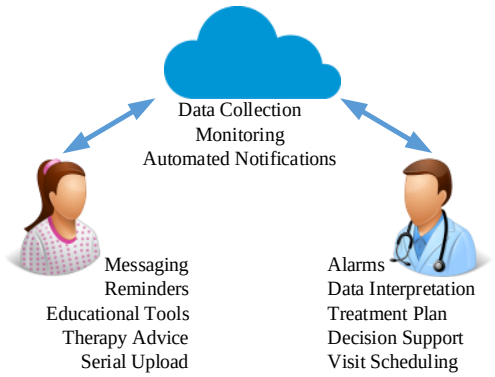

Figure 3. Communications and functions of the main components of IoT infrastructure

Thus, it is possible to describe the healthcare IoT system. The medical device communicates wirelessly with a reader. This reader through the access point load the taken indications for service in the Cloud. Hospitals, emergency doctors and health care providers can access this service. Detailed descriptions of the integration of data from the medical device to the Cloud are presented in [8-9].

III. THE QUEUEING THEORY FOR MODELLING OF IOT PROCESSES

A. *Justification of applicability of the Queueing Theory*

In this paper, the queueing systems are those systems at which random service requests from IoT device (customer) are received at random times, while incoming requests are serviced by means of the available service channels [10-11]. Under the flow of service is understood the flow of requests, serviced one after another by one continuously occupied channel (for example, Cloud).

When considering a single serviced device, the proceeding processes can be represented by a Markov stochastic process (chain) with discrete states and discrete time. However, when considering the IoT infrastructure (due to the huge number of devices and the difference in their characteristics), it should be noted that in this case, all flows are simplest, the process occurring in the IoT system is a Markov stochastic process (chain) with discrete states and continuous time.

Obviously, there is a stationary state in this process. It is not necessary to formulate the Kolmogorov equation since the structure is regular, the necessary formulas are given in the reference books [10-11].

B. *Case Study*

Let us describe a hypothetical situation. The hospital, which is part of the IoT infrastructure, receives 3 service

requests from users of the networked insulin pump (for example, results of sugar level planned measurement, request an appointment, statistics on the number of injections). The flow of all requests is the simplest. The average time of receiving a new request from an insulin pump user is 30 minutes (determined by subjective characteristics), *t*. When the request is received, the medical staff begins to process it. The processing time for one request is distributed according to the exponential law and on average is 10 minutes, t_{pr}. At the initial time, there are no requests in the system. It is required to determine the reliability characteristics of this system.

In this way, there are four possible states in this system:

- S_0 – there are no service requests in the system.
- S_1 – there is one service request in the system.
- S_2 – there are two service requests in the system.
- S_3 – there are three service requests in the system.

We will assume that the processes of receipt and processing of requests are homogeneous Markov, simultaneous receipt of several service requests, as well as simultaneous processing are practically impossible. Since all applications are equivalent, from the point of view of the reliability, it does not matter which service request is in the state S_3, it is important that one.

With this in mind, the situation is modelled by the "birth-death" process (Fig. 4).

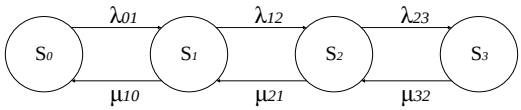

Figure 4. A scheme of "Birth-death" process for the considered case

According to Fig. 4, λ_{01}, λ_{12}, λ_{23} are intensities of service requests flow, μ_{10}, μ_{21}, μ_{32} are intensities of processing flow.

The intensity of receipt of one service request is equal to $\lambda = 1/t$, and the intensity of processing of one request is equal to $\mu_{10} = 1/t_{pr}$.

There are no requests in the state S_0, consequently $\lambda_{01}=3\,\lambda$, in the state S_1 one request was received - $\lambda_{01}=2\,\lambda$, in the state S_2 two requests were received - $\lambda_{01}=\lambda$. In the state S_3 two requests are processing, so $\mu_{10}=3\,\mu$, for the state S_2 $\mu_{21}=2\,\mu$, and for S_1 $\mu_{32}=\mu$.

According to [11] the probability of a state when there are no requests in the system:

$$P_0 = \frac{1}{1+\frac{\lambda_{01}}{\mu_{10}}+\frac{\lambda_{01}\lambda_{12}}{\mu_{10}\mu_{21}}+\frac{\lambda_{01}\lambda_{12}\lambda_{23}}{\mu_{10}\mu_{21}\mu_{32}}} \approx 0.4219 \cdot$$

Similarly, the remaining probabilities are calculated, which are equal to P_1=0.4219, P_2=0.14, and P_3=0.016.

In case of a successful cyber attack on a single vulnerability in the healthcare IoT system the developed "birth-death" model is modified as follows, as shown in Fig. 5.

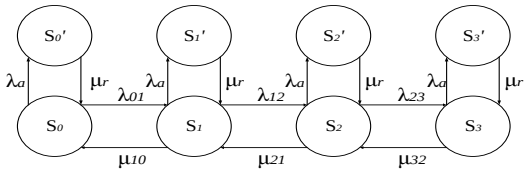

Figure 5. A Markov model for the considered case of a successful attack at one stage of the service request processing (with a halt)

Let us suppose that the successful attack on the healthcare IoT system occurs with a probability of 20% (every fifth attack is successful), and $\mu_r = 0.9$. Let us suppose that at the initial instant of time with a probability 100% is in state S_0. Fig. 6 shows the convergence on the stationary distribution (iterating for 50 steps). The model was simulated using R package "markovchain" [12].

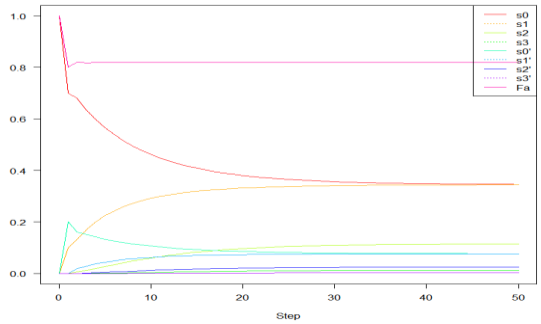

Figure 6. The stationary distribution for the considered case of a successful attack at one stage of the service request processing (with a halt)

If the healthcare IoT system continues to perform its functions without halts during the attacks, in this case an appropriate Markov model is shown in Fig. 7. Fig. 8 shows the convergence on the stationary distribution.

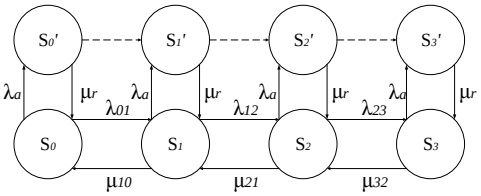

Figure 7. A Markov model for the considered case of a successful attack at one stage of the service request processing (without halts)

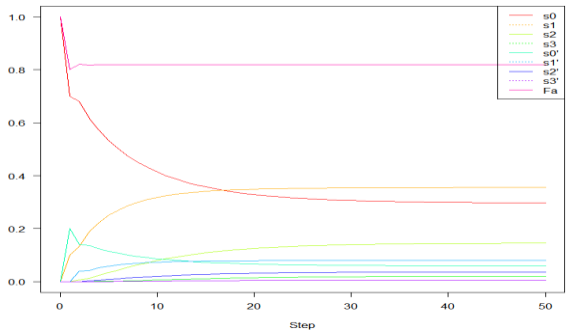

Figure 8. The stationary distribution for the considered case of a successful attack at one stage of the service request processing

In the cases discussed above, the vulnerabilities are not eliminated, and the system just restarts and continues to function in the same way. Fig. 9 illustrates a case when the healthcare IoT system has one vulnerability is eliminated (with $\mu_r' = K_\mu \cdot \mu_r$, $K_\mu < 1$, $t_r' > t_r$). Fig. 10 shows the convergence on the stationary distribution.

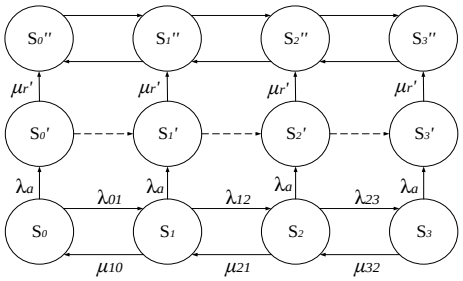

Figure 9. A Markov model for the considered case of a successful attack at one stage of the service request processing (with halts and eliminating of one vulnerability)

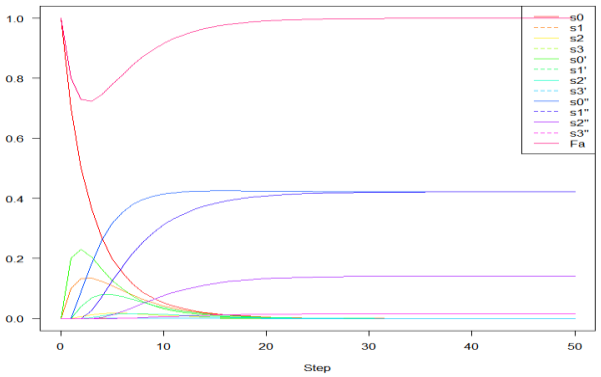

Figure 10. The stationary distribution for the considered case of a successful attack at one stage of the service request processing (with halts and eliminating of one vulnerability)

For the cases depicted in Fig. 5 and 7, the availability functions are calculated as:

$$F_a(t) = P_{s_0}(t) + P_{s1}(t) + P_{s2}(t) + P_{s_3}(t), \quad (1)$$

and for Fig. 9 as:

$$F_a(t) = P_{s_0}(t) + P_{s1}(t) + P_{s2}(t) + P_{s_3}(t) + \\ + P_{s_0}''(t) + P_{s_1}''(t) + P_{s_2}''(t) + P_{s_3}''(t) \quad (2)$$

Analysis of obtained results shows that when one vulnerability is eliminated, the healthcare IoT system has a higher probability to be operational than just restarting, however, the t_r' value affects the duration of the availability function transition period to a stationary mode. For the case depicted in Fig. 9, the availability function falls below due to loss of availability for removing vulnerabilities ($t_r' > t_r$) and then increases to a steady value (after removing vulnerabilities, the healthcare IoT system becomes more secure and reliable).

IV. Conclusions

In this paper, we discussed opportunities and prospects for the IoT application in the field of healthcare and medicine providing. We then analysed the existing healthcare IoT infrastructure. The paper includes the justification of applicability possibilities of the queueing theory and presents the case study for modelling considered IoT system. As a result, using the presented models, it is possible to calculate availability function at the stationary and nonstationary states.

In summary, we observe that the rapid development of a large of portable healthcare devices in the context of IoT, like insulin pumps, are enabling new step of care in which remote monitoring and care become a key feature for enforcing safety.

Next steps of our research will be dedicated to developing new more sophisticated models associated with influence of different kinds of vulnerabilities (both hardware and software vulnerabilities) of the healthcare IoT system (including Cloud, networked healthcare device, communication channels and human factor).

References

[1] Reality Check. *50B IoT devices connected by 2020 – beyond the hype and into reality*. www.rcrwireless.com/20160628/opinion/reality-check-50b-iot-devices-connected-2020-beyond-hype-reality-tag10.

[2] D. Lund, C. MacGillivray, V. Turner, M. Morales, "Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand", *IDC, Framingham, MA*, 2014.

[3] M. A. Malik, "Internet of Things (IoT) Healthcare Market by Component (Implantable Sensor Devices, Wearable Sensor Devices, System and Software), Application (Patient Monitoring, Clinical Operation and Workflow Optimization, Clinical Imaging, Fitness and Wellness Measurement) - Global Opportunity Analysis and Industry Forecast, 2014 – 2021," Alied Market Research, 2016, 124 p.

[4] World Healthcare Organization, "*Global report on diabetes*", 2016.

[5] J. Healey, N. Pollard, and B. Woods, "*The healthcare Internet of things: rewards and risks*", Atlantic Council, 2015, 17 p.

[6] U.S. Food and Drug Adminstration, *Classify your device*. www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm2005371.htm

[7] W. M. Sutton, "*Classification overview*," U.S. Food and Drug Adminstration, 2015.

[8] A. Mohan, Cyber Security for Personal Medical Devices Internet of Things. *Proceedings of* the *IEEE International Conference on Distributed Computing in Sensor Systems*, 26-28 May, 2014, pp. 372-374.

[9] Mohan, A., Bauer, D., Blough, D., Ahamad, M., Bamba, B., Krishnan, R., Liu, L., Mashima, D., Palanisamy, B. A Patient-centric, Attribute-based, Source-verifiable Frameworkfor Health Record Sharing. *GIT CERCS Technical Report GIT-CERCS-09-11*, Georgia Institute of Technology, 2009, 10 p.

[10] L. Lakatos, L. Szeidl and M. Telek. "Markovian Queueing Systems," *Introduction to* Queueing Systems *with Telecommunication Applications, Springer US*, 2012, pp 199-224.

[11] J. Sztrik, "Basic Queueing Theory," irh.inf.unideb.hu/~jsztrik/education/16/SOR_Main_Angol.pdf, 2012.

[12] G. A. Spedicato, T. S. Kang., S. Bhargav, D. Yadav. *The markovchain Package: A Package for Easily Handling Discrete*

Markov Chains in R. https://cran.r-project.org/web/packages/ markovchain/vignettes/an_introduction_to_markovchain_package.pdf.