INTERNATIONAL JOURNAL OF RESEARCH AND ANALYSIS IN SCIENCE AND ENGINEERING

Web: https://www.iarj.in/index.php/ijrase/index

9. Reliability Modeling for Sensor Systems

Subair P. H.
Rtd. HOD, Dept. of Electronics,
SSM Polytechnic, Tirur, Kerala.

Basheer P. I.
HOD, Dept of Electronics,
SSM Polytechnic College Tirur, Kerala.

Shajil Ameer V. V.
Lecturer, Electronics Engineering,
SSM Polytechnic College, Tirur, Kerala.

ABSTRACT:

In key developing industries like automotive and industrial, sensor dependability is now one of the most crucial hurdles for widespread use of Internet-of-things data. To model sensor dependability under diverse load circumstances, the research provides a method based on the Bayes theorem. To ensure the system's long-term viability, it has been tested for both hardware and communication problems. Using several handbooks, we were able to anticipate the failure rate of self-designed and self-developed nodes intended for usage in hard settings.

KEYWORDS: Sensor, Reliability, IOT, Sensor System, Reliability Modeling.

Introduction:

Sensitivity and repeatability of sensors used to keep track of various parameters in critical systems are essential for early detection of malfunctions and the implementation of corrective measures to avoid catastrophic failures. It is the goal of this study to model sensor reliability under a variety of load scenarios and to optimise sensor system reliability by utilising many sensors. Satellite propulsion systems, nuclear power plants, and aircraft systems, among other things, can benefit from this form of simulation[1].

This type of system necessitates an ongoing, dependable monitoring system in order to avoid unanticipated failures that could result in significant financial losses as well as negative consequences for the environment, human health, and safety. A high-reliability sensor system with enough redundancies may be a better option than spending a lot of money on replacing or repairing industrial systems because of unreliable sensors.

Models of sensor reliability under various loading circumstances are attempted to be developed in this paper. There is also a proposed algorithm for determining the most cost-effective mix of sensor types to achieve the desired level of sensor system reliability.

Using a functionally linked output, a sensor can be read by an observer or an electronic instrument to determine a physical quantity. Sensors can be classified as physical, chemical, biological, or electrochemical based on the process by which they translate a certain input into an output. To facilitate transmission, storage, and reading, most sensors produce an electrical output. Sensing element and sensor are terms that are commonly used interchangeably. However, the most advanced sensors are made up of a variety of components[2].

Sensor systems that use built-in compute resources to conduct predetermined operations upon the detection of a certain input and then process data before passing it on are one example of this. Figure 9.1 shows a block diagram of a working sensor system, which consists of four distinct parts: a sensing element that responds electrically when stimulated by external factors; a signal conditioning element that modifies and processes the electrical signal so that the receiver can understand it; and a sensor interface that allows the device to acquire, store, and communicate with an external interface

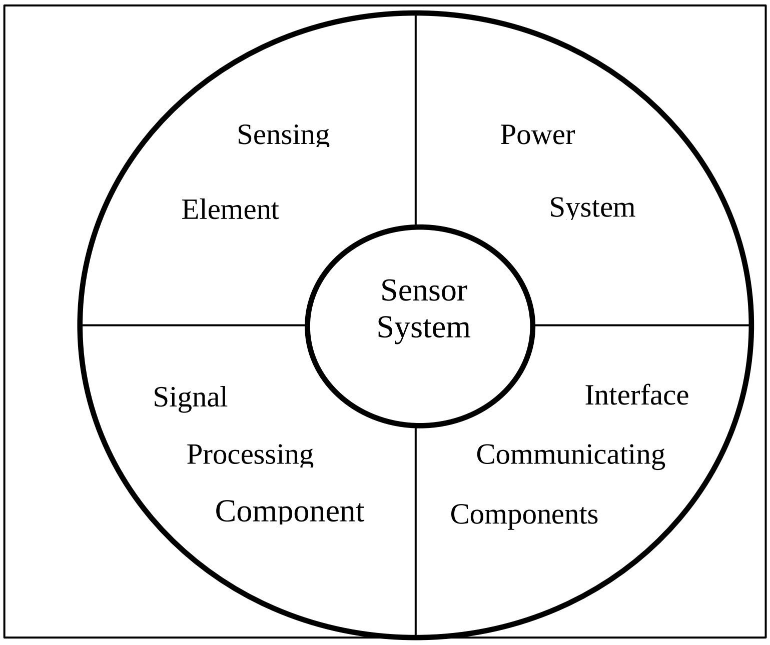

Figure 9.1: A schematic of a sensor system

For self-correcting problems like missing data packages and data collision, the loss of a network element is an essential reliability-related concern in autonomous systems. One possible answer is to construct real-time prediction models that are as strong and long-lasting as possible.You can use a variety of approaches to assess sensor dependability. A total error band figure can be used to analyse the dependability of each particular issue, as well as the overall reliability of a system. Sensitivity, range, precision, resolution, accuracy, offset, linearity, dynamic linearity, hysteresis, and reaction time are all essential considerations. Probabilistic and statistical data are used in the evaluation of sensor dependability.[3-5]

Resistant under specific conditions over a predetermined time period, sensors can be considered reliable when they are capable of delivering the desired results as mentioned above. A sensor's reliability will be heavily dependent on its age, context, and application because of these factors. It is difficult to determine the dependability of sensors while developing new sensors or selecting sensors. When a sensor system is highly dependable in one application, it can suddenly become faulty in a different one[6]. Complex and smart sensor systems (e.g. Sensor Fusion), highly integrated miniature sensor systems (e.g. MEMS/NEMS sensors), long term monitoring requirements (e.g. Condition Monitoring), and high consequence/Mission Critical applications are all examples of applications where high reliability is critical, as illustrated in Figure 9.2. (e.g. High Temperature High Pressure in Oil &Gas fields). Many elements, including sensor design materials selection, manufacturing and packaging process, maintenance and calibration, and the sensor operating environment, must be taken into account when predicting the sensor system's remaining life span.

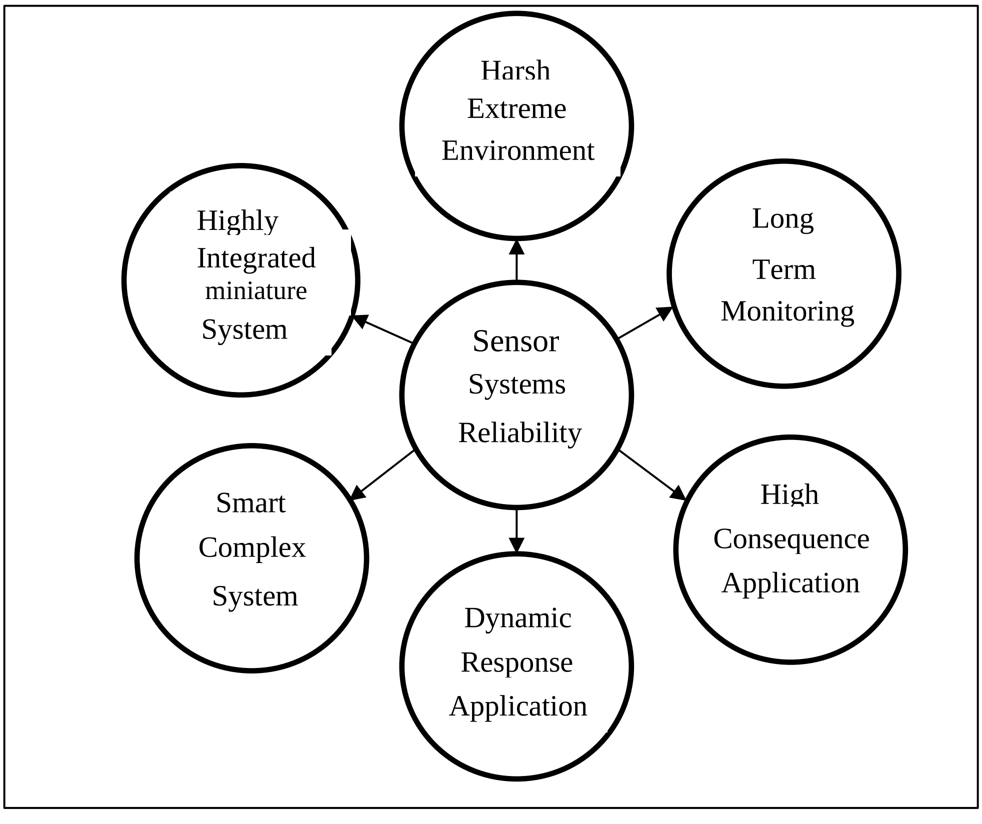
Harsh Extreme Environment
Highly Integrated miniature System
Long Term Monitoring
Sensor Systems Reliability
Smart Complex System
High Consequence Application
Dynamic Response Application

Figure 9.2: Application scenarios where sensor system reliability is extremely important

Review of Literature:

In 2011 Cisco anticipated that there would be 50 billion gadgets connected to the IoT by 2020 (Evans 2011). (Evans 2011). In light of these massive claims, several experts have predicted that by 2020, global investments will be in the trillions of dollars (Rayes and Salam 2016). While these data imply a very rapid rise in IoT, there are still many research issues which must be overcome for IoT to become fully incorporated into our day-to-day lives. Trust, security, interoperability, dependability, scalability, performance, availability, and mobility are some of the issues that stand in the way (Al-Fuqaha et al. 2015; Wang 2018; Ahmed et al. 2017; Saini 2016).

These topics constitute key research issues that must be addressed if we are to allow IoT to become the ubiquitous technology that it has set out to become (Sicari et al. 2016). (Sicari et al. 2016). If the vision of IoT is to be fully implemented in our homes, cities and workplaces then we will be trusting intelligent systems to make thousands of decisions daily that will have profound impact on our lives, through applications such as; home security (Ghorbani and Ahmadzadegan 2017), providing healthcare services to patients (Da Li et al. 2014) and monitoring critical traffic infrastructure (Singh et al. 2014). (Singh et al. 2014). The Internet of Things (IoT) must take into account devices that may be severely restricted by the laws of nature (Chiang and Zhang 2016).

Considering that the IoT will be responsible for managing key infrastructure such as traffic lights, critical health systems and home security, it is easy to appreciate how the impact of unreliable IoT infrastructure may affect the decision-making of the system in a potentially severe or fatal manner (Fekade et al. 2017). (Fekade et al. 2017). The dependability issue does not end at the device and hardware layer either, there is also the question of the reliability of the network layer. Due to its heterogeneous structure and how it transmits data, frequently wirelessly via lossy channels, it might be difficult to verify this. Data transfer is only the beginning of the considerations that need to be made. The vulnerabilities of IoT devices are becoming a big issue in the consumer and government industries. Government guidelines for smart-home devices were published by the UK government in October 2018 to ensure customer safety (DDCMS 2018). This shows that in order for the Internet of Things to completely mature, it will be necessary to address system stability in a comprehensive manner. Because of this, we will be able to utilise the quantified reliability metric to determine whether or not our crucial IoT infrastructure is fit for purpose when we can accurately quantify how reliable our IoT infrastructure is.

Objectives:

Wireless sensor networks' dependability modelling and analysis are reviewed in this article.

Research Methodology:

The existing wireless sensor network reliability modelling works are identified and classed based on several criteria, such as scope, topology, communication paradigms, designs, and reliability evaluation methodologies. There is also discussion of patents that contribute to the reliability of wireless sensor networks.

Result and Discussion:

Sensor Reliability Assessment:

To evaluate sensor dependability in critical developing applications, such as self-driving cars, a model-based architecture for expressing essential sensor parameters is one option[7]. Sensor characteristics and sensor lifetime are examples of functional parameters, which can be determined from monitoring operations (see Figure 9.3).

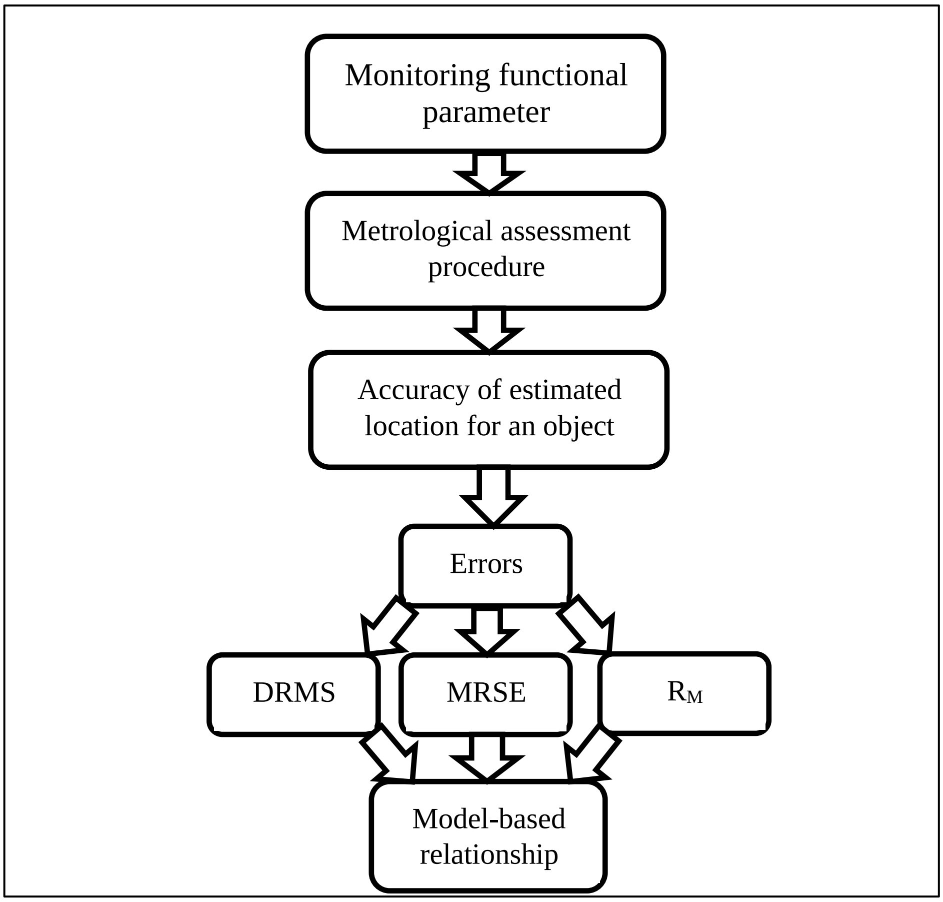
Monitoring functional parameter
Metrological assessment procedure
Accuracy of estimated location for an object
Errors
DRMS
MRSE
R_M
Model-based relationship

Figure 9.3: Procedure for sensor reliability assessment using a model-based approach for sensor data and key performance indices.

It is imperative that automated driving systems (ADS) show that they are sufficiently safe to be used on public roads. If the vehicle's components are reliable enough to allow the driver to safely use them, then the vehicle's safety has been demonstrated in a typical car[8]. To demonstrate the reliability of an ADS, the system's sensors and sensor fusion must be shown to be accurate. Typically, cameras, lidar, and radar sensors are used in today's ADS, each having their own advantages and disadvantages, and all of them merely provide measurements of the environment. As a result, it is critical to be able to establish and quantify the requirements for the dependability of each sensor's perception.

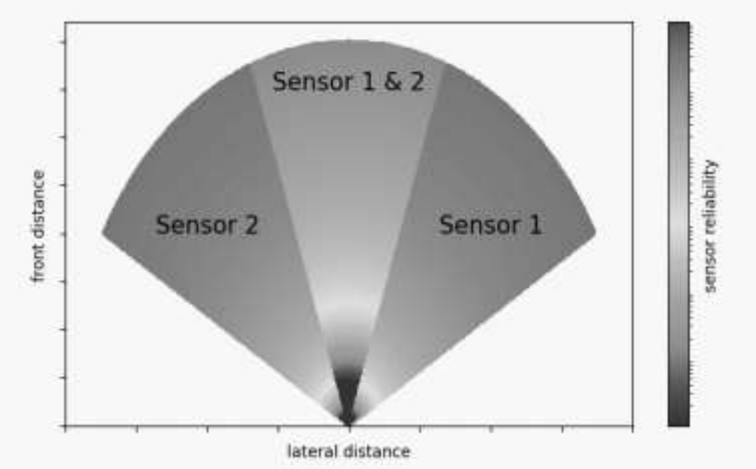

Figure 9.4: automated driving systems

Prediction of Sensor System Reliability:

The term "digital downhole" refers to the complete instrumented drill string, sensor communication, and digital twin model [6]. A more "intelligent" drill string system will be needed if drilling operations in oil and gas are increasingly complicated, deeper, or more hostile (think horizontal drilling and fracking) in order to be safe, economical, and efficient. Sensor systems are used to monitor and report on the conditions in the ground for the benefit of the operations staff. Pressure sensors, flow sensors, and other types of sensors are all important[9-11].

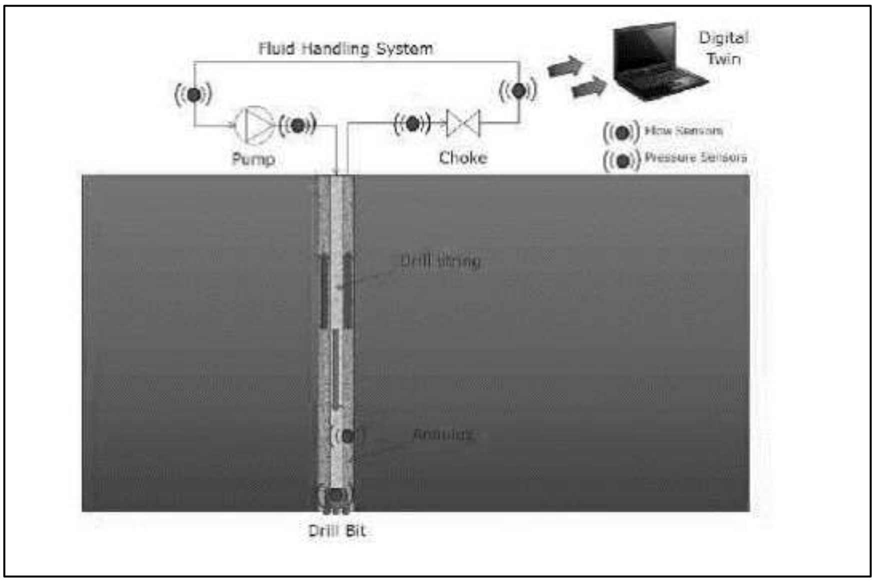

Figure 9.5: The Digital Downhole instrumented by pressure and flow sensors, in this example, reporting data back to update the Digital Twin at the operational station

Constraints may be breached if a pressure pump sensor fails, for example. As with the bit nozzle plugging, the pattern of broken restrictions will be unique if debris plugs the nozzle. Because of the analytical redundancy relations contained in the digital twin that manages sensor data, the constraint matrix will be able to fingerprint many forms of system failures[12].

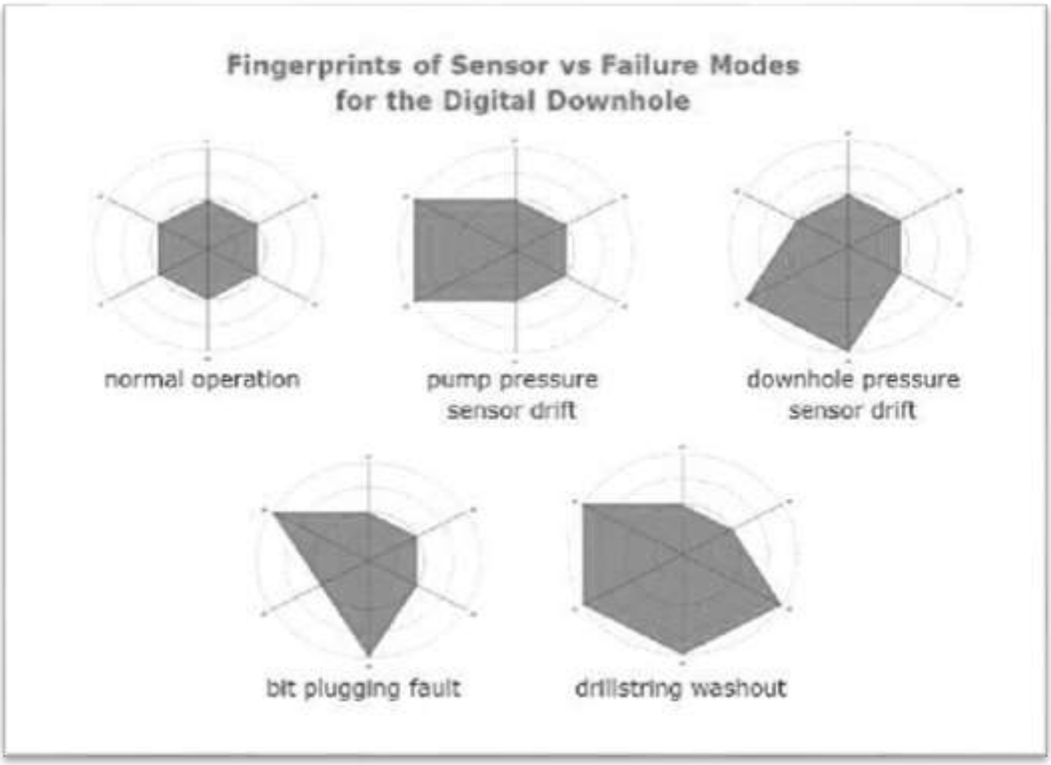

Figure 9.6: Each failure mode for the downhole system corresponding to a unique pattern of deviation in analytical redundancy relations can be used as fingerprints that allow fault detection and isolation within the Digital downhole system

Conclusion:

The robust design and resilient operation of wireless sensor networks are made possible by a large body of work that has been recommended for reliability modelling and analysis. As a result, there's still a lot of room for improvement when it comes to wireless sensor networks and the creation and expansion of key applications that rely on them. Almost every industry has to deal with the problem of sensor system reliability, which is both difficult and crucial. Sensor systems will become increasingly important in all areas of modern industry and society over the next decade since their use is predicted to grow at a rate of more than 10% each year. Sensors that are implanted or left in place in working environments are becoming more common. Eventually, exposure to the operational conditions degrades the sensor systems' reliability. Sensor system reliability threats must, therefore, be carefully assessed.

References:

1. Li, Z.; Kang, R. Strategy for reliability testing and evaluation of cyber physical systems. In Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management, Singapore, 6–9 December 2015; pp. 1001–1006.
2. Vo, M.-T.; Thanh Nghi, T.T.; Tran, V.-S.; Mai, L.; Le, C.-T. Wireless Sensor Network for Real Time Healthcare Monitoring: Network Design and Performance Evaluation Simulation; Springer International Publishing: Cham, Switzerland, 2015; pp. 87–91.
3. Cacciagrano, D.; Culmone, R.; Micheletti, M.; Mostarda, L. Energy-Efficient Clustering for Wireless Sensor Devices in Internet of Things. In Performability in Internet of Things; Springer: Berlin/Heidelberg, Germany, 2019; pp. 59–80.
4. Azghiou K., El Mouhib M., Koulali M. An End-to-End Reliability Framework. Sensors. 2020;20:2439. doi: 10.3390/s20092439.
5. Wang C., Xing L., Zonouz E., Vokkarane V.M., Lindsay Y. Communication Reliability Analysis of Wireless Sensor Networks Using Phased-Mission Model. Qual. Reliab. Eng. Int. 2017;33:823–837. doi: 10.1002/qre.2060.
6. Catelani M., Ciani L., Bartolini A., Guidi G., Patrizi G. Standby redundancy for reliability improvement of wireless sensor network; Proceedings of the 2019 IEEE 5th International Forum on Research and Technology for Society and Industry (RTSI); Florence, Italy. 9–12 September 2019.
7. A.B. Sharma, L. Golubchik, and R. Govindan, “Sensor faults: Detection methods and prevalence in real-world datasets”, ACM Transactions on Sensor Networks (TOSN), 6(3), 2010.
8. F. Ayello, S. Jain, N. Sridhar and G.H. Koch, “Quantitative Assessment of Corrosion Probability – A Bayesian Network Approach”, Corrosion, vol. 70, 2014. [5] S. Guan, F. Ayello, A. N. Sánchez, V. Khare, and N. Sridhar, “Internal Corrosion Direct Assessment using Bayesian Networks Modeling with Limited Data: A Case Study”, CORROSION/2016 paper #7078, NACE International, Houston, TX, (2016).
9. S. Guan, C. Taylor, and N. Sridhar, “Understanding Sensor System Reliability”, DNV GL Position Paper, 2016-2.K.Veeramachineni, L.A. Osadciw, “Biometric sensor management:tradeoffs in time, accuracy and energy,” IEEE Trans.Vol.3, No.4,December 2009.
10. S. Arold and Balanba, “Allocation of system reliability,”, Tech.Rep.,ASD-TDR-62-20, 1962.
11. “Reliability and Maintainability Engineering,” ‘Charles E. Ebeling’.McGraw-Hill International Editions 1997.
12. Li, F., Nastic, S., Dustdar, S.: Data quality observation in pervasive environments. In: Proceedings—15th IEEE International Conference on Computational Science and Engineering, CSE 2012 and 10th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, EUC 2012, pp. 602–609 (2012)
13. Nomm, S., Bahsi, H.: Unsupervised anomaly-based botnet detection in IoT networks. In: Proceedings—17th IEEE International Conference on Machine Learning and Applications, ICMLA 2018, pp. 1048–1053 (2019)
14. Sinche, S., Polo, O., Raposo, D., Femandes, M., Boavida, F., Rodrigues, A., Pereira, V., Sa Silva, J.: Assessing redundancy models for IoT reliability. In: 19th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2018, pp. 14–15 (2018)