# ReFIT: Reliability Challenges and Failure Rate Mitigation Techniques for IoT Systems

Sukanta Dey(✉), Pradeepkumar Bhale, and Sukumar Nandi

Department of Computer Science and Engineering,
Indian Institute of Technology Guwahati, Guwahati 781039, Assam, India
{sukanta.dey,pradeepkumar,sukumar}@iitg.ac.in

**Abstract.** As the number of Internet-of-Things (IoT) devices increases, ensuring the reliability of the IoT system has become a challenging job. Apart from the emerging security issues, reliable IoT system design depends on many other factors. In this work, for the first time, we have shown all the reliability challenges of an IoT system in details, which may arise due to the random faults. We have also proposed a mathematical formulation of the lifetime of the IoT system. Subsequently, we devise an algorithm which uses Lévy distribution-based duty cycling approach to improve the IoT network lifetime. We have validated our proposed method using Cooja simulation software. The simulation results show 1.5 × increment in network lifetime for the IoT system using our proposed method than the state-of-the-artwork. We have also demonstrated that our proposed method does not degrade the network performance.

**Keywords:** Duty cycle · Internet-of-Things · Lévy flight · Lifetime · Low power · Reliability · VLSI

## 1 Introduction

With the inception of Industry 4.0, the human race is experiencing a new age revolution, where all the devices, things, and equipment are connected and controlled with the help of the internet. The establishment of the Internet of Things (IoT) in the industrial sector, has enabled the industry in the automatic, intelligent, and digitalized decision-making process over the internet with wireless components. It has also allowed the industry to perform time-critical cyber-physical operations [1] over the internet. Works related to IoT-based frameworks, its requirements, and its architectures are started to gain attention, which is described in work [2].

Different IoT nodes, for example, smartphones, smart cameras, wearable, house electronics, electric vehicles, smart door lock, garden irrigation systems, can be connected wirelessly to form an IoT network. An illustrative example of IoT nodes forming an IoT network is shown in Fig. 1. These IoT nodes are,

S. S. Rautaray et al. (Eds.): I4CS 2020, CCIS 1139, pp. 123–142, 2020.
https://doi.org/10.1007/978-3-030-37484-6_7

in turn, connected to the sink/border router, through which the IoT nodes are connected to the internet. From this illustrative example, it is clear that for the successful functioning of the IoT system, it is essential for the proper functioning of every IoT nodes. However, the nodes near to border router remain active most of the time and discharge a large amount of energy. Due to which the battery lifetime of the nodes near to border router is decreased. This problem is termed as *energy hole* problem. In this work, we have proposed a solution to address this energy hole problem and to increase the battery-operated lifetime. Apart from that, for the successful deployment of the IoT system, it is also necessary to study different reliability challenges for an IoT system. Therefore, we have also considered various reliability issues for an IoT system and formulated an analytical expression for lifetime calculation.

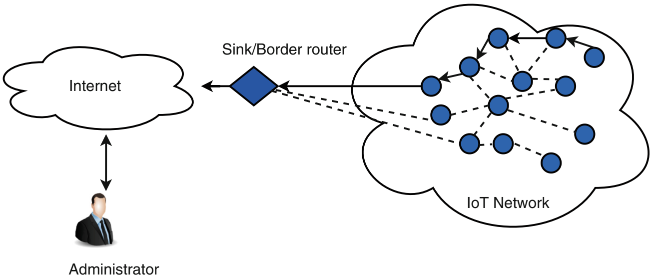

**Fig. 1.** An illustrative example of IoT system

**Motivation:** As the critical autonomous decision making depends on the IoT system, ensuring the reliability of the IoT system has become essential. The objectives of the reliable IoT system should be (1) provide seamless connectivity (2) long-lasting IoT system (3) non-stop working of the IoT system. Without these objectives, the aspiration of Industry 4.0 can not be fulfilled. Considering that, the study of reliability challenges of these IoT systems is very much necessary. Further, the reliability study of the IoT system also helps in designing reliable systems. It also helps in providing seamless and non-disruptive communication among the IoT devices of the system. Further, it is also necessary to alleviate any runtime reliability issues which may arise in an IoT system to increase the lifetime of the IoT system. Therefore, our work focuses on the reliability study of the IoT system, considering various factors. The major contribution of the paper,

- Different reliability challenges for Low Power IoT nodes and systems are discussed in detail in this paper. An analytical expression for mean-time-to-failure (MTTF) calculation of the IoT system is formulated for considering different parameters.
- A Methodology using Lévy Distribution-based duty cycling approach is proposed to decrease the failure rate and to improve the lifetime of the IoT nodes and systems.

- The proposed methodology is validated using simulation with the help of Cooja tool in Contiki OS. The obtained results show that the lifetime increases using our proposed approach.

The rest of the paper is arranged in the following way. The background of the paper is explained in Sect. 2, which contains a brief description of low power IoT nodes, and the previous related work. The reliability challenges of IoT node and systems are mentioned in Sect. 3. Mathematical modeling for the reliability prediction of the IoT system is also discussed in the section. The proposed methodology using a Lévy flight-based duty cycling technique for lifetime improvement of the IoT system is discussed in Sect. 4. The experimental results are listed in Sect. 5. The work is concluded in Sect. 6.

## 2 Background

A pictorial representation of a low power IoT node is shown in Fig. 2. A significant characteristic of the low power IoT node is that all the components of the IoT node should consume low power, and the power supply range must be less than 1 V.

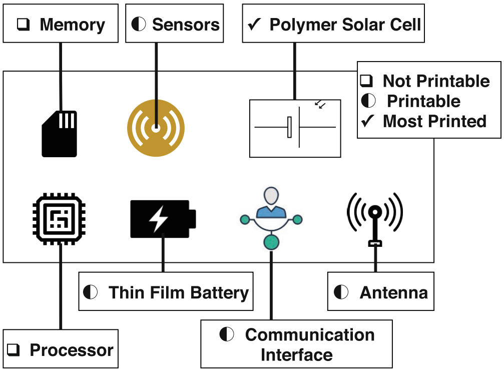

**Fig. 2.** An ideal IoT node with different components [3]

### 2.1 Low Power IoT Nodes

A low power IoT node contains, the following components,

- processor: used to process the data of the IoT node.
- memory: used to store the data.
- thin-film battery: used as the power supply to the IoT node.
- communication interface: used for communication with the hardware.

- antenna: used for communication with the other IoT nodes.
- sensor: used for collecting data.
- polymer solar cell: alternative non-conventional power source.

These are essential components of low power IoT nodes. Some of these components are printable, and some are not printable. For the seamless connectivity of the IoT system, all these components of IoT nodes must work correctly. Any transient or permanent damage to any of the parts due to random faults may create risk for the proper functioning of the IoT system.

## 2.2 Related Works

There are very few works that discussed the reliability challenges of IoT nodes and systems. Most of the papers in the literature concentrate more on the cyber-security perspective of the IoT. There are few works which tried to enhance the IoT network lifetime by giving solution from the security perspective.

A few works which deal with the reliability issues of IoT systems are trying to demonstrate the reliability measures of the IoT systems using different metrics. For e.g., Ahmad [4], in his work, proposed a methodology to deal with the hardware and software-based system-level reliability of the IoT. He validated his work on different case studies using hardware and software. Rosing [5], in his presentation, demonstrated different approaches for the reliability and maintainability of IoT systems. Xing et al. [6] have demonstrated the failure analysis of the IoT system, considering the cascade effect of functional dependency. Thomas and Rad [7] have shown different reliability metrics for the IoT car tracking system. No work in the literature has an objective to model the reliability of the IoT system analytically. In this work, we propose an analytical model for measuring the reliability of the IoT system for lifetime estimation.

There are also a few works that try to maximize the lifetime of the IoT system using different heuristics. Raptis et al. [8] in their work proposed an offline centralized solution of integrated service in order to increase the network lifetime considering latency constraints. They evaluated the performance of their approach using testbed. Valls et al. [9] in their work proposed solutions for the allocation of bandwidth and resources for the data processing using the IoT network, which is used for lifetime maximization. Morin et al. [10] has done a comparative study of the lifetime of different devices in the IoT wireless network. Airehrour et al. [11] in work has done a detailed survey on different energy optimization techniques of IoT nodes using the energy harvesting method. Fafoutis et al. [12] have demonstrated a real-world experiment on the lifetime prediction of the battery for the IoT devices. Cao et al. [13] have proposed an offline solution of mobility-aware network lifetime maximization under quality-of-service (QoS) constraints. Li et al. [14] have intended to improve the IoT network lifetime by introducing the hierarchical cluster-based duty cycle approach. Our proposed method works on top of the framework proposed in [14].

## 3 Reliability Challenges in IoT

IoT systems can fail due to the one or more of the following reasons:

- Due to system-level random failure
    - Errors caused by user.
    - Errors while installation.
    - Problems in communication interface or with the transceiver.
    - Problems with the sensor.
    - Issues with the power (Battery lifetime).
    - Software or firmware failure.
    - Hardware failure (Memory and processor)
        - Soft errors (transient in nature)
        - Hard errors (permanent in nature)
- Due to intended cyber attack on the IoT systems
    - Cyber attack can cause all the system-level failures mentioned above.

These problems may arise due to different attacks by the attacker on an IoT system, which reduces the reliability of the IoT system. Without any pertinent attack by an attacker, the problems mentioned above still can occur, due to some random faults, which also reduces the reliability of the IoT system. Therefore, our objective is to mathematically model the reliability of the IoT system, depending on different parameters. Once the mathematical model is formed, then we can analyze the IoT system in order to reduce the above issues and to increase the lifetime of the IoT system. In this work, we assume that we are not proposing any solution to prevent different attacks on the IoT. However, we are concentrating on those reliability issues which may occur due to random faults.

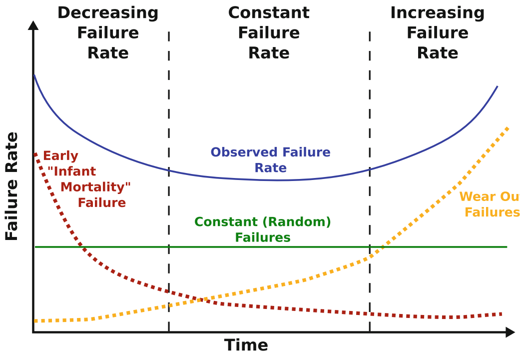

**Fig. 3.** Reliability Bathtub curve.

### 3.1 Mathematical Modeling of Reliability of IoT System

These errors can occur in any of the IoT nodes, which in turn can affect the total IoT network/system. The occurrence of these errors can happen during any instance of its lifetime. Therefore, depending on these issues, the reliability of the IoT nodes and system can be defined as the time-varying function $R(t)$. It defines the probability function that an IoT node operates correctly in time $[0, t\}$. Mean-time-to-failure(MTTF) of the IoT node can be defined as the following:

$$MTTF_{IoT\ Node} = \int_0^\infty R(t)dt \tag{1}$$

Generally, the reliability of any device is modeled with the reliability bathtub curve, as shown in Fig. 3. The bathtub curve is divided into three parts with respect to the lifetime of a certain design of a device. In the first part, the infant mortality rate keeps on decreasing from an initial higher value. When the infant mortality of rate decreases, the lifetime of the device remains almost constant in the second part of the curve. In the end, due to the wear-out failures, the failure rate increases. From the reliability bathtub curve and a deformed version of Weibull distribution [15], we can obtain a mathematical expression for the reliability of an IoT node by the following:

$$R(t) = e^{(-\lambda_f t)}, \tag{2}$$

where $\lambda_f$ is the constant failure rate of the IoT device, which is determined by observing the failure rate pattern of the IoT devices. From (1) and (2), we get that

$$MTTF_{IoT\ Node} = \frac{1}{\lambda_f} \tag{3}$$

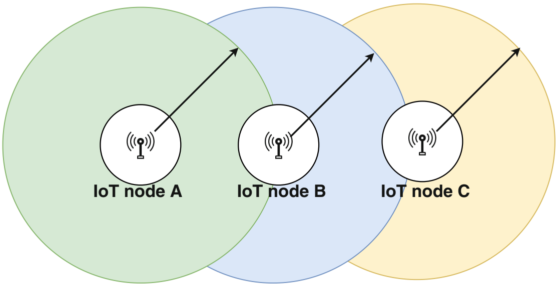

**Fig. 4.** IoT nodes A, B, and C are in series

To obtain the lifetime of the IoT system, we have to observe the connections of the IoT nodes. Considering the IoT nodes are connected in an ad-hoc network mode. If the $n$ IoT nodes are connected in series (as shown in Fig. 4) then all the nodes must work correctly in order to keep the system in working condition. In this case, MTTF of the IoT system is defined as follows,

$$MTTF_{IoT\ Series\ System} = \int_0^{\infty} \prod_1^n R_i(t)dt \tag{4}$$

$$= \frac{1}{\sum_{i=1}^{n} \lambda_{f_i}} \tag{5}$$

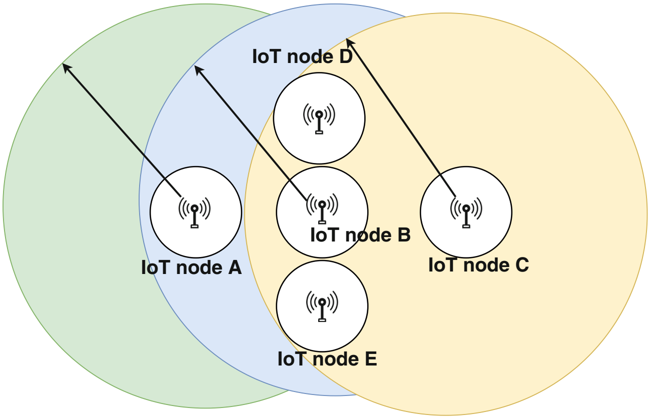

**Fig. 5.** IoT nodes B, D, and E, are in parallel. If all the three nodes, B, D, and E fail, then no communication between node A and C is possible. As a result, the IoT system fails.

If the $n$ IoT nodes are connected in parallel (as shown in Fig. 5) then the IoT system fails if the all the IoT node fails, then rate of failure $F_s(t)$ is defined by the following,

$$F_s(t) = \prod_1^i F_i(t), \tag{6}$$

where $F_i(t) = 1 - R_i(t)$. Therefore, the MTTF of a parallel IoT system is given by,

$$MTTF_{IoT\ Parallel\ System} = \int_0^{\infty} (1 - F_s(t))\, dt \tag{7}$$

However, in reality the IoT systems are neither series system or parallel system. Real IoT system forms a hybrid combination of the series and parallel systems. Therefore, the MTTF of real IoT system can be defined as follows:

$$MTTF_{IoT\ System} = \int_0^{\infty} \prod_1^i R_i(t)dt + \int_0^{\infty} (1 - F_s(t))\, dt, \tag{8}$$

where it is assumed that $i$ devices are connected in series and another $i$ devices are connected in parallel.

### 3.2 Modeling Constant Failure Rate, $\boldsymbol{\lambda_f}$

MTTF of the IoT system can be obtained if we know the constant failure rate, $\lambda_f$. The value of $\lambda_f$ depends on many factors. If the number times a IoT node is used by the user is $K$ in an hour, then the number of errors caused by the user can assumed to be in the order of $log(K)$ in an hour. $\lambda_f$ is directly proportional to $log(K)$.

$$\lambda_f \propto log(K) \tag{9}$$

If the IoT node is running on uniform duty cycle mode, the let $d$ times be the number of time device is turned on in an hour. $\lambda_f$ is directly proportional to $d$.

$$\lambda_f \propto d \tag{10}$$

$\lambda_f$ also depends on the temperature of the devices as mentioned in the Black's equation [16] and Arrhenius equation [17].

$$\lambda_f \propto e^{(-\frac{E_a}{kT})} \tag{11}$$

Due to the negative bias temperature instability(NBTI) and hot carrier injection (HCI) of the underlying semiconductor devices present in the memory and the processor [18]. The failure rate of the these components directly depends on the number of times the write operation ($w$) in the memory is done in an hour.

$$\lambda_f \propto w \tag{12}$$

Due to power supply noise and electromigration also failure can happend in the processor [19,20], which directly depends on the current density($J$) of the IoT node

$$\lambda_f \propto J \tag{13}$$

From the above equations, we have got that the

$$\lambda_f = Clog(K)de^{(-\frac{E_a}{kT})}wJ \tag{14}$$

where $C$ is a proportionality constant. Equation (14) is an analytical expression of the failure-rate calculation.

### 3.3 Mitigation Techniques of Failure Rate

The failure rate can be mitigated by decreasing those terms of (14), which is directly proportional to the failure rate. The failure rate can also be decreased by increasing those parameters, which are inversely proportional to the failure rate. Different solutions can be proposed to mitigate the failure rate by considering various parameters, and the lifetime of the IoT system can be evaluated accordingly. Some of the parameters are inter-dependent, i.e., if one parameter increases, then the other parameter decreases. For such settings, a trade-off between the parameters has to be maintained in order to reduce the failure rate.

In this work, we are only considering the failure of the IoT system due to IoT network failure, which can occur due to the battery failure or discharging of the power sources. The *network lifetime of IoT system* can be defined as given in Definition 1. It is to be noted that the network lifetime of the IoT system is different from the MTTF expression formulated earlier. The MTTF is the mean-time-to-failure of the IoT system, which can be caused by random faults. However, MTTF also depends on the network lifetime, as mentioned in Remark 1. In this work, we are only considering the network lifetime improvement for an IoT system.

**Definition 1.** *When one of the nodes of an IoT system fails to work properly due to the discharge of its battery power, then the time elapsed from the beginning of communication to the first node failure is termed as* ***network lifetime of an IoT system*** *($T_{Nlifetime}$).*

*Remark 1.* The network lifetime of an IoT system is directly related to the MTTF caused by random faults. In other words, network lifetime is related inversely to the failure rate of an IoT system.

*Proof.* If $p$ is the probability of failure of the power system of IoT network, then we can establish a relationship between $T_{Nlifetime}$ and MTTF.

$$T_{Nlifetime} = p * MTTF \tag{15}$$

If random faults occur in the power supply system of IoT network (meaning $p = 1$), then the IoT network fails. For such a case, MTTF can be equivalent to the network lifetime. Therefore, from this, we can see that MTTF and network lifetimes are related. It also implies that network lifetime and failure rate ($\lambda_f$) of an IoT system are related. As MTTF and $\lambda_f$ are inversely related. Hence, $T_{Nlifetime}$ and $\lambda_f$ are inversely related to each other.

In the next section, the proposed methodology for failure rate mitigation is described.

## 4 Proposed Methodology for Failure Rate Mitigation

### 4.1 System Model

We are considering $n$ nodes for our IoT network. These $n$ nodes are connected to the internet via border router. The nodes are clustered hierarchically, as shown in Fig. 6. The nodes are clustered in different layers with a cluster head node for each cluster. Cluster heads are responsible for the communication to the successive layers. The nodes which are near to the border router drain out its energy quickly. Our system model of hierarchical clustering is similar to one the used in [14]. We also adapted the energy model used in [14].

In this work, we propose to improve the lifetime of the IoT system by incorporating an adaptive duty-cycling approach on the similar system model and energy model as used in [14]. We have used Lévy distribution for our proposed adaptive duty-cycling approach.

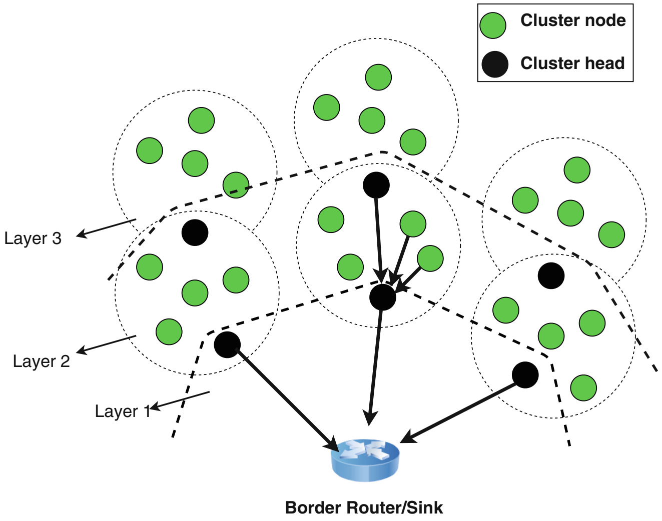

**Fig. 6.** Hierarchical clustering of nodes.

### 4.2 Problem Formualation

Our objective here is to improve the network lifetime of the IoT nodes and systems, which can be mathematically interpreted as

$$\text{maximize} \quad T_{Nlifetime}$$

However, energy constraints of the IoT nodes need to be satisfied. In order to improve the network lifetime we can formulate the same problem in terms of failure rate, $\lambda_f$. As $T_{Nlifetime}$ and $\lambda_f$ are inversely related to each other as showed in Proposition 1. Therefore, we have to minimize the constant failure rate, $\lambda_f$ for increasing the IoT network lifetime. Mathematically it can be represented as,

$$\underset{d_i}{\text{minimize}} \quad \lambda_f$$

$$\text{subject to} \quad E_i(d_i) \leq e_i, \; i = 1, \ldots, m.$$

where $d_i$ represents the layer ID, $E_i(d_i)$ represents the energy consumed by the nodes of the $d_i$ layer, and $e_i$ is the maximum energy allowed in $i^{th}$ layer. We use an adaptive duty cycle-based approach using Lévy Distribution which is described in next.

### 4.3 Lévy Distribution and Lévy Flight

The Lévy distribution is heavy-tailed stable distribution used extensively in the probability theory. The distribution can be approximated as follows [21],

$$L(d) \sim d^{-1-\beta} \tag{16}$$

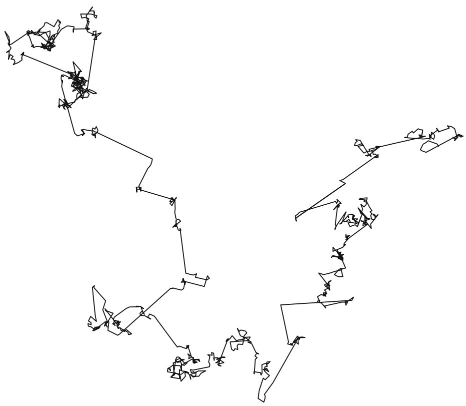

**Fig. 7.** An illustrative example of Lévy flight with $\beta = 1.5$ for 1000 steps

where $0 < \beta < 2$ and $d$ is the distance vector. A random walk which follows the Lévy distribution is known as Lévy flight. An illustrative example of Lévy flight is shown in Fig. 7. From the figure we can see that Lévy flight is a combination of walks with many small step-sizes and few large step-size which follows heavy-tailed distribution. We can use the concept of Lévy flight to obtain the duty cycling of the IoT nodes.

### 4.4 Proposed Lévy Distribution-Based Duty Cycling

Our proposed algorithm for failure-rate mitigation is mentioned in the Algorithm 1. We have used Lévy distribution to obtain the duty cycling of the IoT nodes. We have used similar energy models and system models for our work, as used in [14]. Our objective is to use the duty cycle ratio of the nodes optimally in order to decrease the system failure rate and to increase the system's lifetime. Therefore, initially, the nodes are hierarchically clustered, and to obtain the duty cycles of each node; we use the Lévy flight strategy. The nodes which are nearer to the sink (border router) uses the Variable duty cycle ratio, which corresponds to the Lévy flight strategy. The duty cycle varies similar to the Lévy distribution such that after a series of many small duty cycles, it exhibits fewer larger duty cycle. This methodology helps in reducing the energy hole problem and increases the lifetime of the IoT system without decreasing the system performance. The algorithm is summarized in the Algorithm 1. From the algorithm, we can see that initially hierarchical clustering is done IoT node containing clusters are placed in different layers ($i = 1, 2, \cdots, n$). Subsequently, a random number is generated using Lévy distribution to obtain the duty cycle ratio ($T_r$) of the nodes near to the border router. If the energy required for this duty cycle ratio ($E(T_r)$ ) is less than the stored energy of the nodes ($E(T_{left})$), then the communication keeps on happening, else if $E(T_r) \geq E(T_{left})$ the communication stops and the IoT system fails. The lifetime is calculated depending on its time elapsed from the beginning.

**Algorithm 1.** Proposed Lévy Distribution-based Duty Cycling

```
IoT Nodes are partitioned with hierarchical clustering with clusters placed in
different layers ($i = 1, 2, \cdots, n$), as shown in Fig. 6 ;
while IoT nodes near to border router active do
    Generate a random number ($r$) using the Lévy distribution;
    Duty cycle ratio ($T_r$) $\leftarrow r$;
    if $E(T_r) < E(T_{left})$ then
        Communication happens in IoT nodes;
    else
        IoT System fails;
    Calculate the lifetime;
```

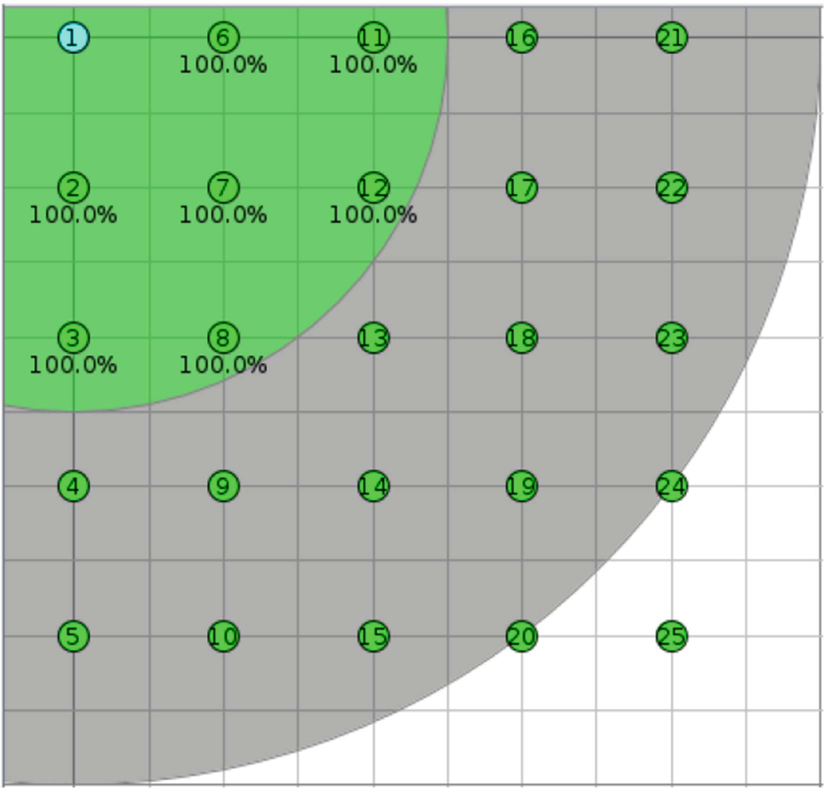

**Fig. 8.** Radio environment of 25 nodes used in simulation with Cooja simulator

# 5 Experiments and Results

## 5.1 Experiments Setup

The evaluation of the proposed methodology for failure rate mitigation and lifetime improvement is done using real hardware parameters of the IoT systems.

**Table 1.** Experimental setup for the Cooja simulator

| Item name | Value |
|---|---|
| Operating system | Contiki 3.0 |
| Simulator | Cooja |
| Target area | 100 m × 100 m |
| Radio environment | UDGM |
| Node type | Tmote Sky |
| Routing protocol | RPL |
| Adaptation layer | 6LoWPAN |
| Transmitter output power | 0 to 25 dBm |
| Receiver sensitivity | 94 dBm |
| Radio frequency | 2.4 GHz |
| Mobility scenario | Random distribute, No mobility |
| Simulation duration | Variable |

The simulation is performed in Contiki Operating System-based Cooja simulator in a machine with Intel i5 processor. We have done our simulation for 15 nodes, 20 nodes, and 25 nodes for the evaluation of lifetime of the IoT system. The experimental parameters are fixed, as mentioned in [14]. The simulation parameters for the Cooja software is done as given in Table 1. The radio environment of the simulated nodes of the Cooja simulator are shown in Fig. 8.

The average power consumption of all the 25 simulated nodes for uniform duty cycling is shown in Fig. 9. The initial duty cycle ratio for all the 25 nodes are shown in Fig. 10. From Figs. 9 and 10, we can get an idea about the average power consumption of the IoT nodes and its duty cycle ratio used initially.

### 5.2 Results and Discussion

We have implemented the Algorithm 1 in the Cooja simulation tool to obtain the effects of the proposed Lévy flight-based duty cycling approach. Accordingly, duty cycles are varied adaptively using the Lévy distribution, and for that, the codes are modified in the Cooja simulation software, and simulations are performed. We also compare our results with the hierarchical clustering approach of EnergyIoT [14] and the uniform duty cycling approach. Comparative representation of the duty cycles used in all the three methods mentioned is shown in Fig. 11. In [14], the authors have utilized the energy consumption in the idle listening in the network construction phase and data processing phase, which saves energy and increases the IoT network lifetime. In our method, the energy consumption in idle listening is utilized with the help of Lévy distribution, which saves the energy much more than the EnergyIoT. The minimum required active time for proper operations of the IoT node is ensured while assigning the duty cycle using the Lévy distribution.

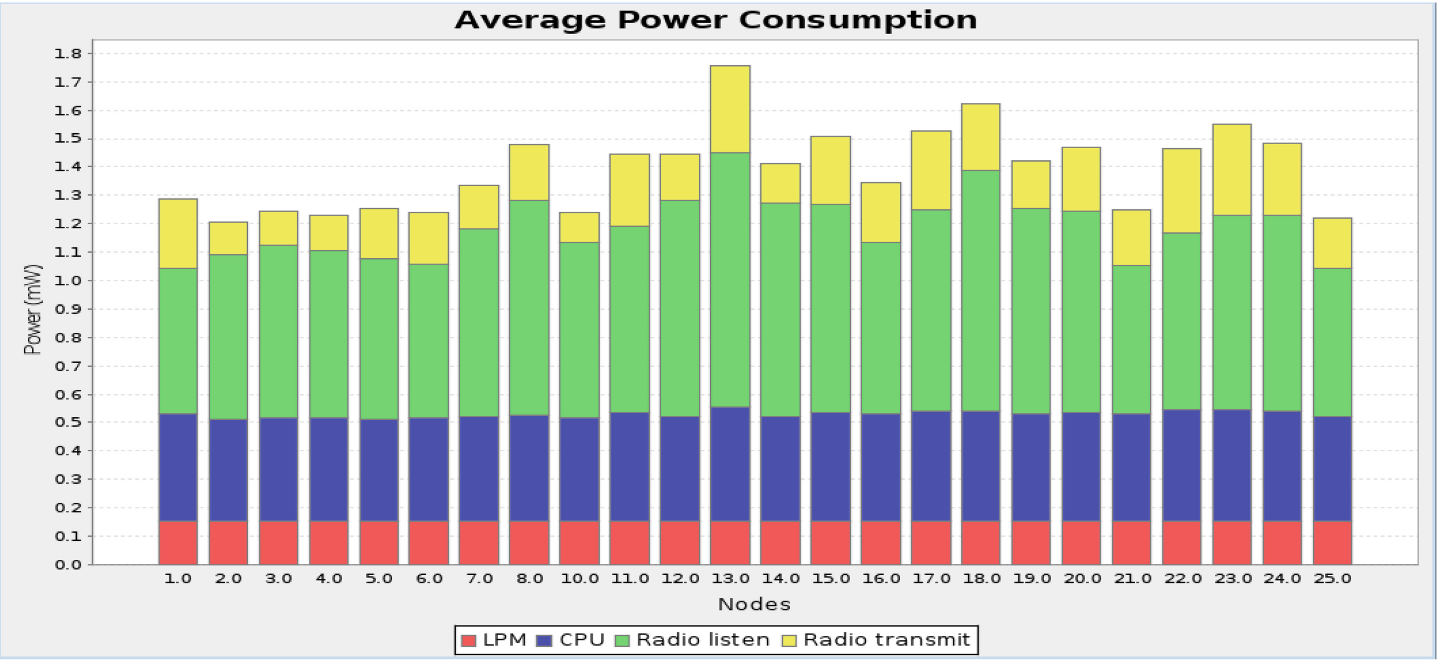

**Fig. 9.** Average power consumption of 25 nodes used in simulation with Cooja simulator.

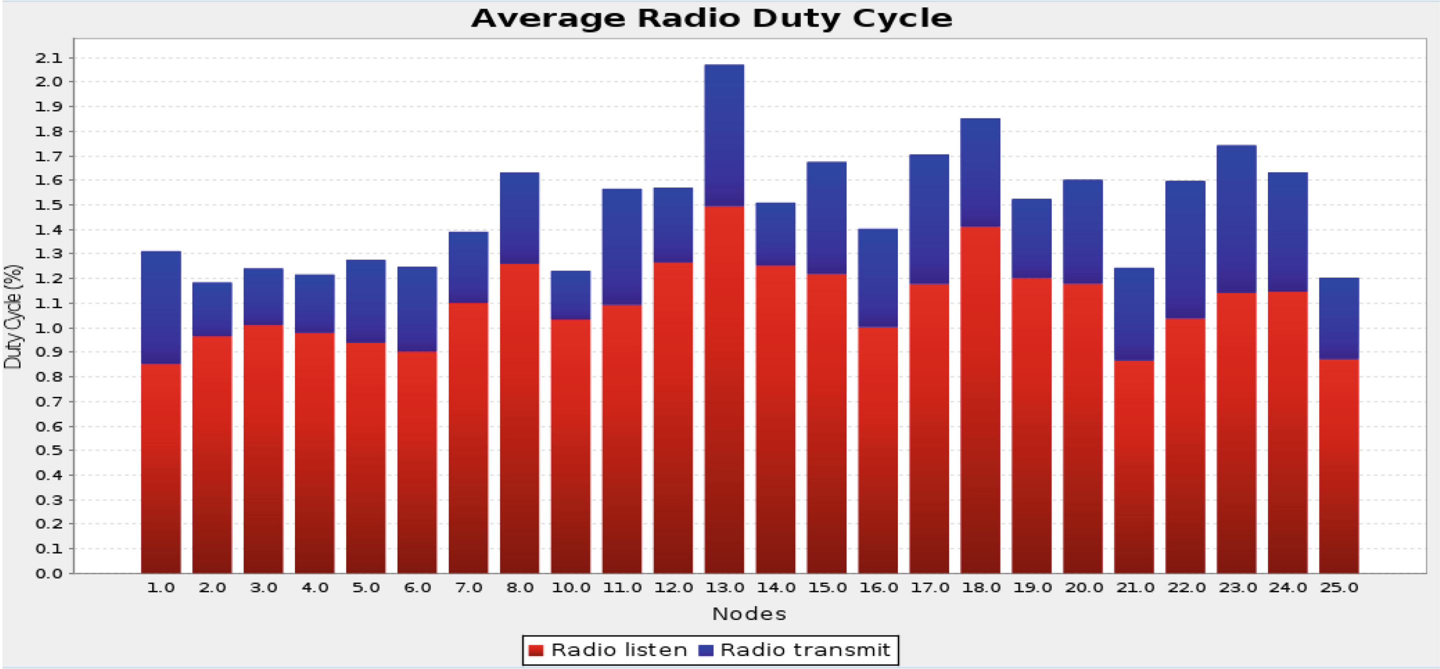

**Fig. 10.** Duty cycle ratio of 25 nodes used in simulation with Cooja simulator.

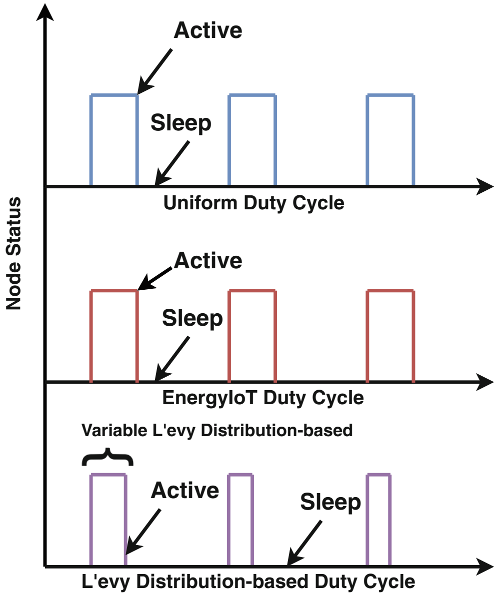

**Fig. 11.** Comparison of duty cycles used in uniform duty cycle, EnergyIoT method and our proposed method.

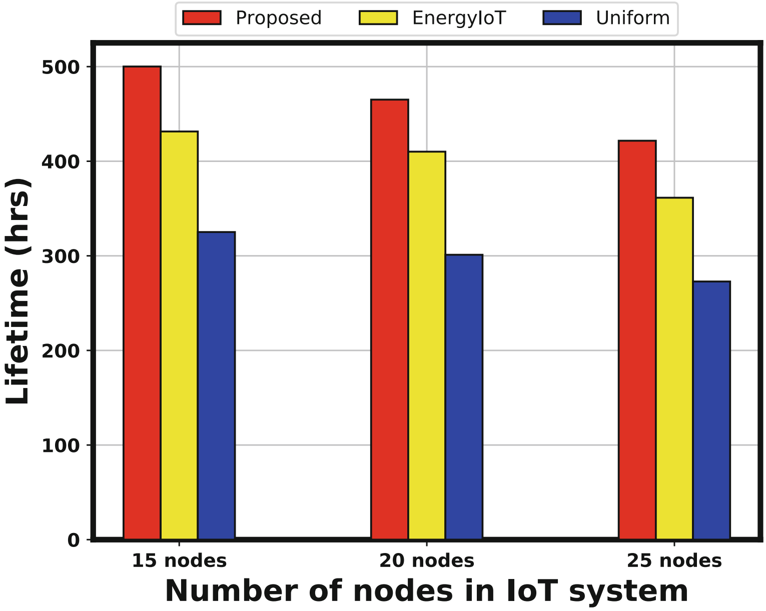

**Fig. 12.** Comparison of the lifetime the variation of nodes in the IoT system.

**Comparison of Lieftime:** The result of the comparison of the lifetime of the IoT system is shown in Fig. 12. From the experiment, we have obtained that the lifetime obtained by our proposed method is longer than that of [14] and a uniform duty cycling approach. One of the main reasons behind this, we have used Lévy flight-based duty cycling, which helps in the reduction of the failure rate of the node near to border router, which helps in the increase in lifetime. It can also be observed from Fig. 12 that when the number of nodes increases, then the lifetime of the IoT system decreases. The increase of lifetime implies the decrease in failure rate.

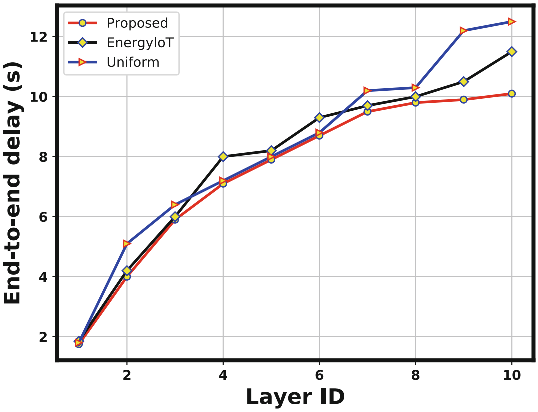

**Fig. 13.** Variation of end to end delay for different layers

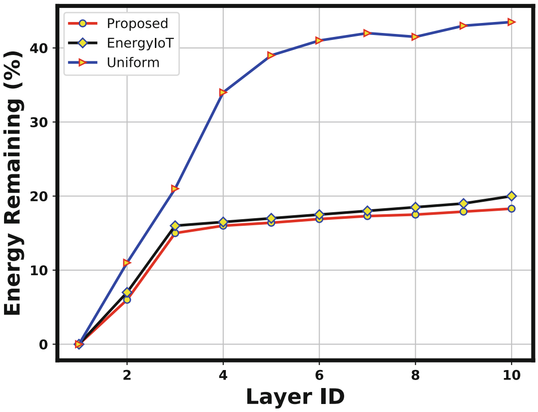

**Fig. 14.** Percentage of energy remaining for different layers

**Network Performance Evaluation:** We have also evaluated the performance of the network for our proposed approach. For that, we have evaluated the end-to-end delay for each of the layers for the 25 node configuration. We have also evaluated the remaining energy for each of the layers. We compare these parameters with the work of [14] and the uniform duty cycling approach. From the result, it can be seen that our approach does not degrade the end-to-end delay as compared to [14], as shown in Fig. 13.

The percentage of energy remaining for different layers of the IoT system is also similar using our approach compared to the [14], as shown in Fig. 14. Therefore, using our Lévy flight-based duty cycling the approach we have gained an increase in the lifetime of the IoT system without degrading the network performance, as shown in this section.

## 6 Conclusion

In this paper, we have studied different reliability challenges in IoT system design due to random faults. We have proposed an analytical expression for the lifetime evaluation of IoT systems. We observe that the lifetime depends on the failure rate. We have also introduced an algorithm using Lévy distribution-based duty cycling to improve the network lifetime and to decrease the failure rates of the IoT system. We have validated our work using the Cooja simulation software. The results demonstrate that the lifetime using our proposed method increases than the state-of-the-art works. Our results also include that lifetime improvement has been achieved without any degradation in network performance. We have also observed that as the number of nodes increases in the IoT systems, the network lifetime decreases. From our work, for designing a reliable IoT system following recommendation should be followed,

- The IoT nodes must use a low duty cycle ratio for its transceivers in order to save battery power.
- The operating temperature of the IoT system should be as low as possible.
- Few numbers of hardware operations should be performed for a better lifetime.
- IoT network with a small number of nodes should be designed with a border router (sink node) for each of the IoT networks.

In the future, a much better adaptive duty cycling scheme can be proposed in order to improve the IoT network lifetime further.

**Acknowledgements.** The work is done as a part of the project title “Information Security Research and Development Centre (ISRDC)” under Information Security Education and Awareness (ISEA) Project (Phase-II) at IIT Guwahati. The authors would like to thank Ministry of Electronics and Information Technology (MeitY) and IIT Guwahati for the support.

## References

1. Wollschlaeger, M., Sauter, T., Jasperneite, J.: The future of industrial communication: automation networks in the era of the internet of things and industry 4.0. IEEE Ind. Electron. Mag. **11**(1), 17–27 (2017)
2. Lucas-Estañ, M.C., Raptis, T.P., Sepulcre, M., Passarella, A., Regueiro, C., Lazaro, O.: A software defined hierarchical communication and data management architecture for industry 4.0. In: 2018 14th Annual Conference on Wireless On-Demand Network Systems and Services (WONS), pp. 37–44. IEEE (2018)
3. Shao, L., et al.: Compact modeling of thin film transistors for flexible hybrid IoT design. IEEE Des. Test **36**, 6–14 (2019)
4. Ahmad, M.: Reliability models for the Internet of Things: a paradigm shift. In: 2014 IEEE International Symposium on Software Reliability Engineering Workshops, pp. 52–59. IEEE (2014)
5. Rosing, T.S.: Reliability and maintainability of IoT systems (2018)
6. Xing, L., Zhao, G., Wang, Y., Mandava, L.: Competing failure analysis in IoT systems with cascading functional dependence. In: 2018 Annual Reliability and Maintainability Symposium (RAMS), pp. 1–6. IEEE (2018)
7. Thomas, M.O., Rad, B.B.: Reliability evaluation metrics for Internet of Things, car tracking system: a review. Int. J. Inf. Technol. Comput. Sci. (IJITCS) **9**(2), 1–10 (2017)
8. Raptis, T.P., Passarella, A., Conti, M.: Maximizing industrial IoT network lifetime under latency constraints through edge data distribution. In: 2018 IEEE Industrial Cyber-Physical Systems (ICPS), pp. 708–713. IEEE (2018)
9. Valls, V., Iosifidis, G., Salonidis, T.: Maximum lifetime analytics in IoT networks. In: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, pp. 1369–1377. IEEE (2019)
10. Morin, E., Maman, M., Guizzetti, R., Duda, A.: Comparison of the device lifetime in wireless networks for the Internet of Things. IEEE Access **5**, 7097–7114 (2017)
11. Airehrour, D., Gutiérrez, J., Ray, S.K.: Greening and optimizing energy consumption of sensor nodes in the Internet of Things through energy harvesting: challenges and approaches (2016)
12. Fafoutis, X., Elsts, A., Vafeas, A., Oikonomou, G., Piechocki, R.J.: On predicting the battery lifetime of IoT devices: experiences from the sphere deployments. In: RealWSN@ SenSys, pp. 7–12 (2018)
13. Cao, K., Xu, G., Zhou, J., Wei, T., Chen, M., Hu, S.: Qos-adaptive approximate real-time computation for mobility-aware IoT lifetime optimization. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. **38**, 1799–1810 (2018)
14. Li, Q., Gochhayat, S.P., Conti, M., Liu, F.: EnergIoT: a solution to improve network lifetime of IoT devices. Pervasive Mob. Comput. **42**, 124–133 (2017)
15. Weibull, W., et al.: A statistical distribution function of wide applicability. J. Appl. Mech. **18**(3), 293–297 (1951)
16. Black, J.R.: Electromigration–a brief survey and some recent results. IEEE Trans. Electron Devices **16**(4), 338–347 (1969)
17. Laidler, K.J.: Chemical Kinetics, vol. 42. Harper & Row, New York (1987)
18. Guo, X., Verma, V., Gonzalez-Guerrero, P., Stan, M.R.: When "things" get older: exploring circuit aging in IoT applications. In: 2018 19th International Symposium on Quality Electronic Design (ISQED), pp. 296–301. IEEE (2018)
19. Dey, S., Dash, S., Nandi, S., Trivedi, G.: PGIREM: reliability-constrained IR drop minimization and electromigration assessment of VLSI power grid networks using

cooperative coevolution. In: 2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 40–45. IEEE (2018)
20. Dey, S., Nandi, S., Trivedi, G.: PGRDP: reliability, delay, and power-aware area minimization of large-scale VLSI power grid network using cooperative coevolution. In: Mandal, J.K., Sinha, D. (eds.) Intelligent Computing Paradigm: Recent Trends. SCI, vol. 784, pp. 69–84. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-7334-3_6
21. Dey, S., Dash, S., Nandi, S., Trivedi, G.: Markov chain model using lévy flight for VLSI power grid analysis. In: 2017 30th International Conference on VLSI Design and 2017 16th International Conference on Embedded Systems (VLSID), pp. 107–112. IEEE (2017)