Improving Mean Time to Failure of IoT Networks with Reliability-Aware Routing

Kazim Ergun[1], Raid Ayoub[2], Pietro Mercati[2], Tajana Rosing[1]
[1]*University of California San Diego, La Jolla, USA* [2]*Intel Corporation, Hillsboro, USA*

***Abstract*—The unprecedented scale and ubiquity of the Internet of Things (IoT) introduce a maintainability challenge. IoT networks operate in diverse and harsh environments that impose non-negligible thermal stress on the IoT devices with no active cooling. The lifetime of these networks can be limited by the exacerbated effects of hardware failure mechanisms at high temperatures, exponentially accelerating reliability degradation. In this paper, we propose a novel reliability-driven routing approach to mitigate the reliability degradation of IoT devices and improve the network Mean Time to Failure (MTTF). Through routing, we curb the utilization of highly degrading devices, which helps to lower the device power dissipation and temperature and reduce the effect of temperature-driven failure mechanisms. The routing protocol makes the decisions based on the current reliability of the devices, the amount of degradation they will experience due to communication activity, and networking performance. We enhance the ns-3 network simulator to support our reliability modeling and evaluate the routing performance by comparing with state-of-the-art approaches.**

I. INTRODUCTION

The Internet of Things (IoT) continues to rapidly develop as it is adopted progressively across many domains such as logistics, farming, environmental monitoring, healthcare, and smart infrastructures. The number of interconnected IoT devices, or "things", has already exceeded 10 billion and by 2025 it is expected to reach 40 billion. Worldwide spending on the IoT was forecast to be $746 billion in 2019, an increase of 15.4% over the $646 billion spent in 2018, according to a new update from International Data Corporation (IDC) [1]. The inherent large-scale of the IoT unfortunately brings a maintainability challenge, causing a significant portion of operational expenses (up to 80% [2]) to be associated with maintenance costs. While meeting the needs of a growing range of applications, it is also a crucial requirement for IoT devices and networks to operate reliably for long periods, otherwise, maintenance investments can become a critical bottleneck.

Recent advances in energy harvesting techniques combined with energy-efficient approaches at different layers of the networking stack made it possible for IoT devices to have substantially prolonged battery lifetimes. With batteries continuously being recharged by energy harvesting sources, energy-neutral operation [3] for the network can be ensured. In such networks, since the risk of batteries running out of energy is diminished, the limiting factor for network lifetime are hardware failures due to reliability issues. As a result of aging and degradation, components in IoT devices lose reliability and fail, leading to a permanent loss of functionality.

Previous research has shown that reliability degradation of electronics worsens exponentially with increasing temperature due to intensified effects of various mechanisms such as Time-Dependent Dielectric Breakdown (TDDB), Electromigration (EM), Bias Temperature Instability (BTI), and Hot Carrier Injection (HCI) [4]–[6]. The devices composing IoT networks are deployed in harsh environments, resulting in stress on the hardware to reduce the reliability and mean time to failure (MTTF) of devices. The majority of the IoT devices don't have active cooling to mitigate the thermal stress. In such cases, curbing power dissipation of devices helps to lower the device temperatures and scales down the effect of temperature-driven failure mechanisms to achieve a better MTTF. Network routing can be useful in this regard; it is possible to place the IoT devices under thermal stress into low-power states by avoiding them in the communication paths. In this way, low-reliability devices in the network are utilized less to reduce the stress.

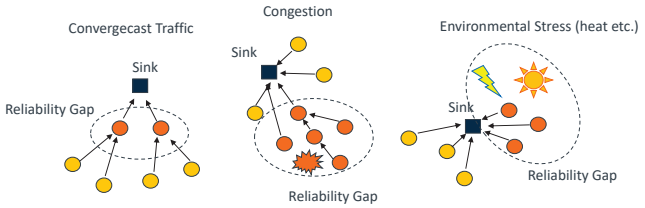

Fig. 1: Reliability problems limiting network lifetime

Many energy-based routing algorithms have been proposed [7]–[9] with the goal of extending the battery lifetime of IoT networks, but no work considers the reliability of IoT devices. It should be noted that we refer specifically to the aging and reliability degradation of the hardware of an IoT device, not to the communication reliability or soft errors. To improve the MTTF of IoT networks, a reliability-aware routing is should be designed following these principles:

1) Avoid the weakest nodes (with a low reliability): As shown in Fig. 1, there are many conditions that may result in an unbalanced reliability degradation in IoT networks. We call this phenomenon *reliability gap*, the situation in which there is a significant reliability difference between different nodes (devices) of the network. Reliability gap can arise as a result of convergecast traffic patterns, congestion, environmental stress, and disproportionate communication distances (Fig. 1a-c). For networks with convergecast traffic patterns and local congestions, some regions in the network have more traffic to forward and hence, the nodes here are 'active' more often than the others. Similarly, some nodes are exposed to higher thermal stress due to the environments networks are deployed in, especially in applications such as industrial and environmental monitoring. These nodes are the bottleneck for the network lifetime since their reliability degrades rapidly, so they are the first to fail because of shortened MTTF. This unfairness problem has to be addressed by the routing protocol so that the networking load can be distributed in consideration with the reliability of the nodes, avoiding weakest nodes.

978-0-7381-3361-4/21/$31.00 ©2021 IEEE

2021 10th Mediterranean Conference on Embedded Computing (MECO) | 978-1-6654-3912-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/MECO52532.2021.9460211

2) Use efficient communication links: If the communication link is of low quality and inefficient, then the transmitter node must send many copies of the same packet to be correctly captured by the receiver. Multiple retransmissions mean that the transmitter and receiver nodes will stay active and experience reliability degradation until a successful reception takes place. Using better links contributes to both the communication performance and device reliability. Therefore, the routing protocol should be aware of the link quality and its influence on device reliability.

In this paper, we propose a novel reliability-aware routing approach to mitigate the reliability degradation of IoT devices and improve the network MTTF. We consider the lifetime of the network as the time at which the first node fails. Hence, we maximize the MTTF of the most degraded nodes by (i) avoiding them in the communication path, (ii) using high quality links to reduce retransmissions. In this way, we obtain a balanced reliability among network nodes.

The contributions of this paper are as follows:

- To the best of our knowledge, we are the first to consider and explore the problem of network routing with the focus on hardware reliability to improve network MTTF.
- We propose a combined routing metric of a node's reliability and its Expected Transmission Count (ETX) [10] over a communication link. Through ETX, we assess the expected link performance as well as the expected reliability degradation for using the given link. Thus, routing decision is made based on the current reliability of the nodes on the path, the amount of degradation they will experience due to retransmissions, and networking performance.
- We enhance the ns-3 network simulator [11] to support our reliability modeling and evaluation mechanism. As an example application of our reliability-based metric, we modify the ns-3 Ad-hoc On-demand Distance Vector (AODV) routing implementation and evaluate its performance by comparing with state-of-the-art approaches.

II. RELIABILITY MODELING

Reliability is defined as the probability of not having failures up to a given time t. The reliability function $R(t)$, in general, can be expressed as a function of *failure rate* $\lambda_f(t)$ [5]:

$$R(t) = e^{-\int_0^t \lambda_f(t')dt'} \tag{1}$$

From Equation (1), the rate of how quickly reliability is changing (degrading) is determined by the failure rate. On the other hand, the value of the failure rate is a function of many parameters, some of which are temperature, time (aging), device power state, and switching frequency between power states.

In our reliability analysis, we focus on hard failure mechanisms that cause irrecoverable device failures. Mechanisms such as Time-Dependent Dielectric Breakdown (TDDB), Electromigration (EM), Bias Temperature Instability (BTI), and Hot Carrier Injection (HCI) induce reliability degradation, and thus eventually cause failures. Failure rate models have been developed for each mechanism, which show a strong (exponential) dependence on temperature, described as follows:

$$\lambda_{device,s} = A_0 \gamma_s e^{-\frac{E_a}{kT_s}} \quad \forall s \in \{active, idle, sleep\} \tag{2}$$

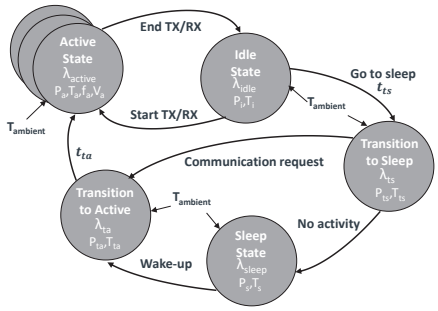

Fig. 2: System model

where A_0 is an empirically determined constant, E_a is the activation energy, k is the Boltzmann's constant, and γ is a constant depending on the respective mechanism and device. Here, we consider temperature T_s of a device as a function of its power state, ambient temperature, and time. When a device switches to a different power state, temperature increases/decreases until it converges to a new steady-state value after a certain time. We assume that the IoT devices can be in various operational states (e.g., $active$, $idle$, $sleep$) denoted s, characterized by power dissipation, voltage, and frequency.

Fig. 2 depicts the diagram of device operational states with the state transition mechanism and the parameters characterizing the states. For IoT devices, switching between power states using duty-cycling and wake-up radio techniques – usually implemented at MAC layer – is common for energy saving purposes [12]. The objective of state transitions (represented with arcs) is to put the IoT device in low power modes when not communicating. In the idle state, the system-on-a-chip (SoC) of the device is powered on but not communicating or processing any packets. In the sleep state, most of the SoC subsystems are power-gated. In the active state, the device is busy transmitting/receiving and processing packets. Power scaling methods such as DVS policies are used for transition between active states for some IoT devices, either down-scaling to reduce power consumption or up-scaling to meet an application performance criteria [3]. Failure rates and the amount of induced reliability degradation change with each power state since different level of power consumption causes a different temperature. Besides, ambient temperature heavily influences the devices internal temperature, which shows its effect in every operational state.

A. Reliability Assessment in Practice

In practical systems, reliability tracking is possible with degradation, stress, and aging monitors. These monitors, based on ring oscillators that convert temperature and voltage stress into oscillation frequency, give statistically significant information on the accumulated stress of the SoC. This information is used to estimate failure rates and reliability degradation caused by different mechanisms (e.g., TDDB, EM, BTI) [13], [14]. As an example use for IoT, the authors in [15] implement an on-chip stress monitor for IoT devices and outline a picture of its future usage in IoT maintenance and management. The system reliability degradation status is usually input into dynamic reliability management (DRM) techniques [16] to improve device usage. In our case, we propose to use it within network routing protocols to improve the network MTTF.

B. Reliability Assessment in Network Simulation

Analytical models for power, temperature, and reliability should be used to enable reliability evaluation and analysis in network simulations. In this work, we leverage the recently proposed *RelIoT* [17] framework for the ns-3 simulator and enhance it according to our reliability modeling discussion. *RelIoT* offers an application-based power model that characterizes power consumptions of different applications running on IoT devices, particularly targeting edge computing scenarios. We modify this and implement a power state machine model as in Fig. 2. The state transitions take place according to node's communication activity. We directly use *RelIoT*'s first order differential temperature model, which incorporates the dependence of node's internal temperature on power and ambient temperature. The model dynamically updates device temperature when ambient temperature changes or a state transition occurs. During the transient period, temperature increases/decreases until converging to the steady-state temperature of the new operational state. Finally, our modified reliability model dynamically updates node's reliability through Equation (3) by recursively subtracting the degradation induced between progressive state transitions. The current implementation exploits the reliability model presented in [6].

$$R_{device,s} = R_{device,s'} - \Big(\underbrace{R(t_{s'}, T_s) - R(t_s, T_s)}_{\text{degradation}} \Big) \quad (3)$$

The subscripts s and $s^{'}$ indicate the current and previous states respectively. T_s is the temperature experienced by the device between two state transitions from time instants $t_{s'}$ to t_s. $R(\ )$ is the static reliability function described in Equation (1).

III. RELIABILITY-AWARE ROUTING

A. Problem Statement

Consider a wireless ad-hoc IoT network with N nodes (i.e, IoT devices) deployed in a mesh topology. The nodes continuously generate data, which needs to be communicated to a sink (i.e., server). Since the network topology is mesh, nodes can cooperate to distribute and relay data in a multi-hop fashion. In such setting, we seek to improve the network's mean time to failure (MTTF) by means of routing, while keeping performance at adequate levels. As stated previously, how quickly a node's reliability degrades depends on its communication activity, which is influenced by routing decisions. MTTF of a single node can be expressed through Equation (4) as a function of reliability.

$$MTTF_{device} = \int_0^\infty R_{device}(t)dt \quad (4)$$

Then, network MTTF is the minimum of any node in the network (i.e. $\min_{i \in N} MTTF_{device,i}$), acknowledging that – as a common definition – a network fails with the first node's failure.

B. Reliability-Based Routing Metric

Our goal is to construct a routing metric that maximizes the MTTF of the most degraded node as well as takes into account the performance. We need a routing metric that satisfies the following properties:

(1) help avoiding paths with the minimum reliability nodes,
(2) utilize efficient communication links,
(3) lead to decisions that will induce minimal reliability degradation.

Thus, we propose a combined routing metric of a node's *reliability* and its *expected transmission count* (ETX) over communication links.

ETX is one of the most frequently used metrics in routing protocols. It estimates the number of data transmissions required to send a packet over a link and get acknowledged, including retransmissions. It is computed as:

$$ETX = 1/(p_{s \mapsto d} \cdot p_{d \mapsto s}) \quad (5)$$

where $p_{s \mapsto d}$ is the probability of successful packet delivery from source s to destination d. Through ETX, we assess the link performance as well as the expected reliability degradation for using that link. To calculate the reliability degradation to be induced, we first estimate the traffic that the node has to forward. Let j denote the node of interest, then the total allocated traffic for j is the sum of traffic it generates and the traffic incoming from its neighbors:

$$TR_j^{total} = TR_j^{gen} + \sum_{i | i \mapsto j} TR_i^{total} \quad (6)$$

Multiplying this estimate of total traffic (TR_j^{total}) with the expected transmission count ($ETX_{j \mapsto}$) and then dividing by the data rate (r_j) of the node, we compute the expected communication time.

$$t_j^{comm} = (TR_j^{total} \cdot ETX_{j \mapsto})/r_j \quad (7)$$

Finally, we estimate the reliability degradation (DEG_j) to be induced by exploiting Equations (1) and (3).

$$DEG_j = R(t_{s,j}, T_{s,j}) - R(t_{s,j} + t_j^{comm}, T_{s,j}) \quad (8)$$

Here, the calculations are carried out for a communicating node, so the device operational state is active ($s = active$). Since DEG is proportional to ETX, its value will be higher for low-quality links. Selecting paths with the minimum DEG utilizes efficient links (better performance with fewer packet loss) and induces minimal reliability degradation. Hence, by including it in our routing metric, property (2) and (3) are satisfied.

As the second part of our combined metric, we need a component that focuses on the bottleneck in network MTTF – the node with minimum reliability – to satisfy property (1). This component is not 'local', in fact, it is a 'global' one because all of the nodes in the network should be considered to find and avoid the minimum reliability node in the path. In that manner, it is not an additive routing metric; the weight of the walk in a path P is calculated through Equation (9) as the minimum reliability between all the traversed nodes. Given a network and a path from source s to destination d defined by the node sequence $s = n_0, ..., n_l = d$, the weight of the walk w_P is:

$$w_P(s, d) = \min_{j=1,...,l} R_{device,j} \quad (9)$$

To complete our routing metric, we combine the degradation and path walk weight components derived in Equations (8) and (9) respectively. Routing protocols conventionally choose the shortest path, that is the one with the minimum routing metric. Thus, we express our routing metric as a weighted combination of degradation and path walk weight, in a 'lower is better' form.

$$\alpha \cdot \max_{j=1,..,l}(1 - R_{device,j}) + \beta \cdot \sum_{j=1}^{l} DEG_j \qquad (10)$$

In this form, both components represent a degradation value. The first term considers the overall degradation experienced by the node in its lifetime up to now. The second term considers the total degradation to be induced to all the nodes on the path with for a given routing decision. Parameters α and β are their respective weights, configurable based on the routing objective.

Using this metric, routing decision is made based on the current reliability of the nodes, the amount of degradation they will experience due to retransmissions, and networking performance (by the use of ETX). Since the metric is not additive and cannot be independently calculated for each node, its computation can vary between different routing protocols, depending on the adopted shortest path algorithm. We demonstrate the AODV implementation in the next section as an example application.

IV. EVALUATION

We conduct simulations based on a hypothetical scenario of environmental monitoring. IoT devices (nodes) are randomly distributed over a field of 1000m x 1000m. They generate Constant Bit Rate (CBR) traffic and transmit UDP data to a sink node in an ad-hoc fashion. Wireless links between nodes are assumed lossy, so successful packet transmission are not guaranteed. All the communication-related parameters used in our simulations are summarized in Table I.

TABLE I: Simulation parameters

Parameter	Value
Simulation Area	1000m x 1000m
Number of Nodes	50
Routing Protocol	AODV, AODV-ETX, AODV-REL
MAC Layer	IEEE 802.11b
Traffic Type	CBR UDP
Data Rate	20,40 kbps
Packet Size	512 bytes
Bandwidth	2Mbps
Loss Model	ns3::HybridBuildingsLossModel

Reliability heavily depends on the temperature of the environment that the device operates, so we consider real, varying ambient temperature conditions. We use a temperature dataset covering 50km x 50km region in Southern California, which contains half-hourly ambient temperature measurements of 210 locations over a year [18]. Moreover, we consider the effects of the device being placed in different places by selecting the temperature as $T_{amb} \pm U(-10, +10)$, where U is a uniform distribution. For example, a device placed in a closed container under the sun, with airflow around the device is restricted, will have much higher ambient temperature than a device placed under a shade in open air. Finally, reliability is evaluated considering TDDB failure mechanism.

All the models and solutions are implemented in the ns-3 network simulator, leveraging *RelIoT* framework [17] for power, temperature, and reliability simulation. We modified the original models in this framework to to support our routing implementation. In the following, we compare our routing approach (referred to as AODV-REL) with the original AODV [19] and AODV-ETX [20].

Table II shows the average results of 20 simulations run with random ambient temperature distribution and randomized link losses. The simulation duration is 600 seconds for each run, but we scaled up the impact of the TDDB degradation mechanism to be able to display the difference in reliability. In terms performance, our approach produces a better packet loss than AODV, which is hop-count based rather ETX-based. Since we also utilize the ETX metric, the performance is closer to AODV-ETX in some scenarios. However, the node with the minimum reliability degrades much higher for both AODV and AODV-ETX. These methods continuously utilize the same nodes on the communication path, rather than distributing the load.

TABLE II: Simulation results

Data Rate [kbps]	Protocol	Minimum Reliability	Packet Loss [%]	Throughput [kbps]
20	AODV	0.32	1.71	19.33
20	AODV-ETX	0.35	0.55	19.82
20	AODV-REL	0.92	1.45	19.63
40	AODV	0.15	4.15	39.19
40	AODV-ETX	0.22	3.28	39.71
40	AODV-REL	0.78	3.66	39.34

V. CONCLUSION

In this paper, we explored the problem of maintaining IoT device reliability from the perspective of network routing. We proposed a metric to improve network MTTF, which helps the routing protocol to make its decisions based on the current reliability of the nodes, the amount of degradation they will experience, and networking performance. As an example application, we modified the ns-3 AODV protocol with our metric and demonstrated improved network MTTF compared to AODV and AODV-ETX methods.

REFERENCES

[1] IDC, "The Growth in Connected IoT Devices," 2019, [Online].
[2] Cisco Jasper, "The hidden costs of delivering iiot services: Industrial monitoring & heavy equipment," Apr. 2016.
[3] Kansal *et al.*, "Power management in energy harvesting sensor networks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 6, no. 4, 2007.
[4] McPherson, "Reliability challenges for 45nm and beyond," in *2006 43rd ACM/IEEE design automation conference*. IEEE, 2006, pp. 176–181.
[5] Rosing *et al.*, "Power and reliability management of socs," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 15, no. 4, pp. 391–403, 2007.
[6] Zhuo *et al.*, "Process Variation and Temperature-Aware Reliability Management," in *Proceedings of the Conference on Design, Automation and Test in Europe*. European Design and Automation Association, 2010, pp. 580–585.
[7] Behera *et al.*, "Residual energy-based cluster-head selection in wsns for iot application," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5132–5139, 2019.
[8] Dhumane *et al.*, "Routing issues in internet of things: a survey," in *Proceedings of the international multiconference of engineers and computer scientists*, 2016.
[9] Zhao *et al.*, "An energy-efficient region-based rpl routing protocol for low-power and lossy networks," *IEEE Internet of Things Journal*, vol. 3, no. 6, 2016.
[10] De Couto *et al.*, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of the 9th annual international conference on Mobile computing and networking*, 2003, pp. 134–146.
[11] "The ns-3 Network Simulator," https://www.nsnam.org/, [Online].
[12] Kozłowski *et al.*, "Energy efficiency trade-off between duty-cycling and wake-up radio techniques in iot networks," *Wireless Personal Communications*, 2019.
[13] Grenat *et al.*, "4.2 increasing the performance of a 28nm x86-64 microprocessor through system power management," in *ISSCC*. IEEE, 2016.
[14] Baranowski *et al.*, "Synthesis of workload monitors for on-line stress prediction," in *2013 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*. IEEE, 2013, pp. 137–142.
[15] Takeuchi *et al.*, "Experimental implementation of 8.9 kgate stress monitor in 28nm mcu along with safety software library for iot device maintenance," in *2019 IEEE International Reliability Physics Symposium (IRPS)*. IEEE, 2019, pp. 1–7.
[16] Mercati *et al.*, "Workload and user experience-aware dynamic reliability management in multicore processors," in *2013 50th ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 2013.
[17] Ergun *et al.*, "Reliot: Reliability simulator for iot networks," in *Internet of Things - ICIOT*, 2020.
[18] NREL, "National Solar Radiation Database (NSRDB)," https://maps.nrel.gov/nsrdb-viewer, [Online].
[19] Perkins *et al.*, "Ad-hoc on-demand distance vector routing," in *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*. IEEE, 1999, pp. 90–100.
[20] Jevtic *et al.*, "Novel etx-based metrics for overhead reduction in dynamic ad hoc networks," *IEEE Access*, vol. 7, pp. 116 490–116 504, 2019.