https://doi.org/10.31891/csit-2026-1-6

UDC 49.33.35

ENERGY–AWARE MODELLING OF IOT NETWORK LIFE–CYCLE UNDER INDUCED FALSE–EVENT FLOWS

Chen YU
Postgraduate Student, Department of Computer Control Systems, Vinnytsia National Technical University, Vinnytsia, Ukraine,
Staff Member, Department of Computer Science, Guangxi Vocational University of Agriculture, Nanning, China,
e-mail: 122190835@qq.com
https:/orcid.org/0009-0002-8974-848X

Viacheslav KOVTUN
DrSc, Professor, Head of the Department of Computer Control Systems, Vinnytsia National Technical University, Vinnytsia, Ukraine,
e-mail: kovtun_v_v@vntu.edu.ua
https://orcid.org/0000-0002-7624-7072

Received: 24/01/2026
Accepted:10/03/2026
Published:26/03/2026

An energy-aware analytical model of the IoT network life-cycle under induced false-event traffic is proposed. The study considers event-driven clustered IoT networks operating under external influences that generate false event messages and thereby cause unnecessary sensing, transmission, reception, and forwarding operations. Unlike conventional approaches that usually treat traffic behaviour, communication energy consumption, and network geometry separately, the proposed model integrates these components within a unified formal framework. Within this framework, the energy cost of a single false event is formalised and linked to the network-level energy balance, false-event arrival parameters, and node mobility. On this basis, closed-form analytical expressions are derived for the temporal evolution of residual energy and for the duration of the network life-cycle under fixed spatial topology. The model thus establishes an explicit relationship between induced false-event intensity and the depletion of network resources. The analysis shows that the intensity and regularity of false-event arrivals significantly affect the degradation trajectory. In particular, more regular induced traffic changes the early-stage depletion pattern, whereas at high intensities different traffic regimes converge. The model is validated by simulation for a LEACH-based clustered IoT network. The simulation results confirm the analytical dependencies over the investigated range 1 ≤ λ_f ≤ 10 and show that the proposed formulation remains in close agreement with the simulation reference. In the comparative analysis, the prediction error of the proposed model remains within about 0%-2%, whereas the traffic-only baseline reaches about 10.2% and the classical LEACH baseline about 20.4%. These results demonstrate that the proposed model provides a more adequate estimate of network life-cycle because it explicitly incorporates induced-loss effects ignored or oversimplified in conventional approaches.

Keywords: IoT networks; false–event traffic; energy–aware modelling; network life–cycle; probabilistic traffic; clustered IoT systems.

Introduction

The rapid expansion of Internet of Things (IoT) infrastructures has intensified the importance of energy efficiency and long–term operability of large–scale sensor networks. In many practical deployments [1–3], IoT nodes operate under strict energy constraints and are expected to function autonomously over extended periods without maintenance or energy replenishment. Under these conditions, external induced influences, such as false–event traffic, can significantly accelerate energy depletion even in the absence of classical cyber–attacks or protocol violations.

Conventional approaches to IoT security and reliability primarily focus on detecting and mitigating explicit cyber intrusions, while the impact of induced false–event flows on the energy life–cycle of the network remains insufficiently quantified [4, 5]. Induced false–event flows are understood in this study as artificially generated streams of event messages triggered by external influences that do not correspond to real physical events in the monitored environment. Such influences may include jamming-induced repeated sensing, fabricated message injection, spoofed sensor readings, malicious activation of compromised nodes, or other adversarial actions that stimulate normal reporting procedures without violating the communication protocol. As a result, the network processes such messages as legitimate events, which causes additional communication activity and accelerates energy depletion. Existing models often treat traffic behaviour, communication energy consumption, and network geometry as largely independent factors, which limits their ability to capture the cumulative effect of induced events on network degradation.

This creates a scientific and practical challenge of developing energy–aware modelling tools capable of linking probabilistic characteristics of induced traffic with communication energy costs and spatial network organisation. Addressing this challenge is essential for predicting the operational lifetime of IoT networks, supporting capacity planning, and designing resilient sensing systems for smart environments, industrial monitoring, and large–scale cyber–physical applications.

The problem statement and review of recent research

Existing analytical approaches to modelling IoT and wireless sensor networks have predominantly focused on energy consumption under legitimate operational conditions. Classical energy models [6–8] accurately describe per-packet transmission, reception, and aggregation costs and are widely applied to estimate network lifetime in clustered architectures such as LEACH. However, these models implicitly assume that traffic is either stationary or fully controlled, and they do not explicitly account for externally induced false–event flows that activate normal communication procedures while remaining indistinguishable from legitimate events. As a result, the cumulative energetic impact of such induced influences is underestimated.

Probabilistic traffic models [9, 10] represent another important class of approaches. Poisson processes and their deterministic counterparts are commonly employed to characterise event arrivals in IoT systems. While these models capture the statistical properties of traffic streams, they are typically decoupled from detailed energy depletion dynamics. Event arrival rates are often introduced only as average load parameters, without analysing how arrival regularity, inter-arrival variability, or sustained triggering affect long-term energy degradation. Consequently, existing probabilistic models fail to quantify the life-cycle reduction caused by continuous false-event activation.

Security-oriented studies [11, 12] largely address explicit attacks, including denial-of-service, jamming, and protocol-level exploitation. These approaches focus on detection, mitigation, or filtering of abnormal traffic patterns and assume observable deviations from legitimate behaviour. Induced false–event traffic does not violate protocol rules and therefore remains outside the scope of most intrusion-detection frameworks. Although such traffic may persist over long periods, its effect on energy depletion is rarely modelled explicitly, leaving a gap between security analysis and energy-aware lifetime assessment.

Geometric and coverage-based models [13–15] provide valuable insights into sensing probability, connectivity, and transmission distances. Nevertheless, these models usually treat geometry as a static background parameter and do not integrate it with probabilistic traffic dynamics or energy consumption mechanisms. As a consequence, they cannot capture how induced false–event flows propagate through spatially distributed networks and translate into system-level energy loss over time.

In summary, existing approaches tend to address energy consumption, traffic behaviour, security, and network geometry in isolation. They lack a unified analytical framework capable of linking probabilistic characteristics of induced false–event flows with communication-energy expenditure and spatial organisation of the network. This fragmentation prevents quantitative assessment of IoT network life-cycle under induced influences and motivates the development of an integrated energetic–probabilistic–geometric model, as presented in this study.

Formulation of the article's objectives

The goal of this study is to develop an energy–aware analytical model of the IoT network life–cycle under induced false–event flows, which integrates probabilistic traffic characteristics, communication–energy consumption, and network geometry into a unified modelling framework.

To achieve this goal, the following objectives are addressed:

1. To formalise the per–event energy cost of induced false events in a clustered IoT network, accounting for transmission, reception, and aggregation at node and cluster–head levels.

2. To derive a network–wide energy balance model that separates baseline consumption under legitimate operation from additional depletion induced by false–event traffic.

3. To integrate false–event arrival characteristics and node mobility into a continuous formulation linking micro–scale energy expenditure with macro–scale life–cycle degradation.

4. To establish an explicit analytical relationship between induced false–event flow parameters and the IoT network life–cycle under fixed spatial topology.

5. To assess the impact of arrival regularity by comparing Poisson and deterministic false–event streams and to validate the resulting life–cycle model through LEACH–based simulation.

Presentation of the main material

This section explores the quantitative dependence between induced false–event flows and the life–cycle of an IoT network. The focus is on evaluating how the arrival rate of false events λ_f and node mobility v jointly determine the depletion rate of the network's collective energy budget. The life–cycle L is defined as the number of operational rounds prior to the exhaustion of the last node's energy. Each round includes five one–second iterations, during which the cluster–head CH set rotates according to the LEACH protocol. Nodes are homogeneous, initialised with $E_0 = 2$ J, and communicate using the standard first–order radio model [86, 105], with $E_{rx} = 50$ nJ/bit and $E_{amp} = 100$ pJ/(bit · m^2). The sink is centrally positioned in a 200×200 m field, and 5 % of nodes act as CHs per round.

The analytical reasoning begins with the energy expenditure of a single false event, which represents the atomic process driving subsequent depletion. When a sensor detects a false stimulus, two transmissions occur: (i) from a member node to its CH and (ii) from the CH to the sink. These transmissions each incur electronic and amplifier losses; the reception at the CH adds an additional receive cost. Summing these yields the per–event energy expenditure:

$$E_{evt}(v) = l\left[\left(E_{tx} + E_{amp} d_{mc}^2\right) + E_{rx} + \left(E_{tx} + E_{amp} d_{cs}^2\right)\right], \tag{1}$$

where l is the packet size (bits), d_{mc} is the mean member–CH distance, and d_{cs} the mean CH–sink distance.

Equation (1) thus formalises the micro–scale energy dynamics of a single reporting cycle; it provides the base from which aggregate consumption for the entire network will be derived.

At the macro–scale, network–wide power loss arises from the collective activity of all N nodes. Since a fraction p of them act as CHs each round, the number of heads is $N_{ch} = pN$. The mean baseline power P_{base} therefore includes both CH transmissions and member transmissions associated with legitimate (non–false) traffic:

$$P_{base} = N_{ch} E_{evt}^{CH} + \left(N - N_{ch}\right) E_{evt}^{mem}. \tag{2}$$

Equation (2) represents the stationary background load of a healthy IoT network without interference. It is crucial for differentiating natural energy consumption from induced losses. Equation (2) can be further specified by decomposing the mean per–event energy into two components: E_{evt}^{mem} for ordinary member nodes and E_{evt}^{CH} for cluster heads. The former represents the transmission energy of a node sending an l–bit packet to its cluster head at a mean distance d_{mc}, expressed as $E_{evt}^{mem} = l\left(E_{tx} + E_{amp} d_{mc}^2\right)$. The latter accounts for the dual role of the cluster head – receiving packets from an average of n_m members and forwarding the aggregated data to the sink at distance d_{cs}: $E_{evt}^{CH} = n_m l E_{rx} + l\left(E_{tx} + E_{amp} d_{cs}^2\right)$. Substituting these into (2) yields the generalised network–wide expression

$$P_{base} = pN\left[n_m l E_{rx} + l\left(E_{tx} + E_{amp} d_{cs}^2\right)\right] + (1 - p) Nl\left(E_{tx} + E_{amp} d_{mc}^2\right),$$

which analytically links the LEACH clustering parameters with the baseline energy consumption of the IoT network.

When false events are introduced, the network experiences stochastic energy perturbations proportional to the event rate λ_f and the mean per–event cost $E_f(v)$. To integrate this external influence into the power balance, the total induced drain (P_{loss}) is defined as

$$P_{loss}\left(\lambda_f, v\right) = \lambda_f E_f(v),\ E_f(v) = \alpha E_{evt}(v), \tag{3}$$

where $\alpha \approx 0.1$ denotes the average proportion of nodes reacting to each false stimulus. This coupling of λ_f with $E_{evt}(v)$ establishes a direct functional dependency between the intrusion process and network energy depletion. Equation (3) thus transitions the analysis from per–event to continuous–flow energy dynamics. A refined analytical expression for $E_{evt}(v)$ can be derived by linking the per–event energy from (1) to the cumulative energy dynamics in (3). In this formulation, $E_{evt}(v)$ represents the average energy expended by the network in response to a single false event, incorporating mobility–related overheads. Analytically, it may be written as $E_{evt}(v) = E_{evt}(0)\left(1 + \beta v^2\right)$, where $\beta \approx 10^{-2}$ s^2/m^2 quantifies additional reclustering and re–routing costs induced by node motion. Substituting this relation into (2) and (3) yields the instantaneous power loss term

$P_{loss}\left(\lambda_f, v\right) = \lambda_f \alpha E_{evt}\left(v\right)$. This analytical coupling transforms the model from discrete per–event accounting to a continuous–flow representation, directly associating the false–event arrival process λ_f and node mobility v with the overall rate of network energy depletion.

The network's cumulative energy over time (t) is subsequently described by a conservation equation combining baseline and induced drains:

$$E_\Sigma\left(t\right) = E_\Sigma\left(0\right) - t\left[P_{base} + P_{loss}\left(\lambda_f, v\right)\right]. \tag{4}$$

Here $E_\Sigma\left(0\right) = NE_0$ is the total initial energy, and the linear subtraction term represents the progressive loss due to communication activity. Equation (4) integrates (2) and (3), translating local stochastic events into a deterministic macroscopic trajectory for network degradation. Its derivative with respect to time provides the instantaneous power loss rate, enabling predictive control of node longevity.

The network lifetime is then derived as the time interval until the energy reservoir is fully depleted, which (after normalisation to round duration Δt) gives

$$L = \frac{E_\Sigma\left(0\right)}{\left[P_{base} + P_{loss}\left(\lambda_f, v\right)\right]\Delta t}. \tag{5}$$

Equation (5) provides the analytical bridge between traffic parameters and survivability. It encapsulates how increases in λ_f (denser false–event flows) or in v (greater mobility and re–clustering) shorten the operational lifetime by elevating the denominator in proportion to cumulative energy drain. The structure of (5) directly underpins subsequent simulation results.

Differentiating (5) yields $\frac{dL}{d\lambda_f} < 0$ for all positive rates and $\frac{dL}{d\lambda_f} \to 0$ as $\lambda_f \to \infty$, indicating a saturation of energy losses at high intrusion intensities. This transition from steep decline to steady–state behaviour is crucial for identifying the threshold beyond which further increases in false traffic no longer yield proportionate degradation.

Experimental Studies

The proposed analytical model was further examined through computational experiments aimed at evaluating the impact of induced false–event flows on the energy life–cycle of an event–driven wireless sensor network. The experimental study focuses on analysing how the intensity of induced false events influences the network lifetime predicted by the derived analytical expressions. For this purpose, a numerical simulation framework was implemented to reproduce the behaviour of the model under different intrusion intensities and mobility conditions. The experiments were designed to illustrate the dependence $L\left(\lambda_f\right)$ predicted by the theoretical model and to analyse the sensitivity of the network lifetime to variations in the rate of induced false events. The obtained results provide a quantitative illustration of the analytical relationships derived in the previous section and serve as a basis for interpreting the behaviour of the system under increasing levels of induced false traffic.

Before Figure 1, we state the computational set–up and notation used in its construction. The curves are generated in MATLAB by evaluating (5) over $\lambda_f \in \left[1, 10\right]$ events•s(^{–1}) for three speeds $v \in \left\{2, 5, 10\right\}$. For each v, $E_{evt}\left(v\right)$ is obtained from (1) with the mobility correction above; d_{mc} and d_{cs} are the mean intra–cluster and CH→sink distances for a LEACH topology on a 200×200 m field with a 5% head–set. Baseline P_{base} is fixed by the legitimate load (same radio model and packet size l as for false events), whereas P_{loss} scales linearly in λ_f via (3). Axes are: False–event rate λ_f and Network life–cycle L; legend indicates node speed v.

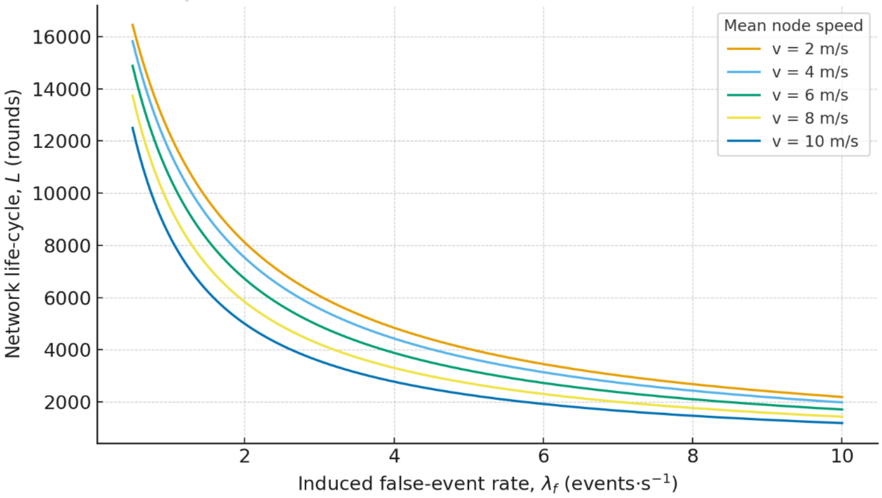

Fig. 1. IoT network life–cycle versus induced false–event rate for different node speeds

The family of decreasing curves exhibits a pronounced initial drop: raising λ_f from 1 to 2 more than halves L. This non–linear sensitivity is predicted by (5) because P_{loss} enters the denominator additively; at low rates, small increments in λ_f produce a large relative increase in total drain. As λ_f exceeds ≈ 4, the slope flattens: $\frac{dL}{d\lambda_f} \to 0$, signalling a saturation regime in which nodes transmit almost continuously and further intensification yields diminishing degradation. Mobility shifts all curves downward, with the largest separation visible at small λ_f: faster motion $v = 10$ increases re–clustering frequency and amplifier usage, effectively inflating $E_{evt}(v)$ through the βv^2 term. At high λ_f, the network is load–saturated regardless of v, so speed becomes a secondary factor. The match between these tendencies and (1)–(5) supports the adequacy of the analytical scaffold for capacity–planning and resilience studies.

Prior to Figure 2, we clarify its aim and computation. The intent is to isolate the effect of arrival regularity on survivability by comparing Poisson versus deterministic false–event streams at the same mean rate and speed. Using the same parameters as above and fixing $v = 2$, we evaluate (5) with identical P_{base}. For the Poisson stream, inter–arrival variability induces idle gaps; for the deterministic stream, arrivals are evenly spaced, eliminating micro–idle opportunities. In the analytical proxy, this difference is captured by the effective utilisation of P_{loss} over each round: Poisson variability yields slightly lower effective utilisation at small λ_f, whereas deterministic timing drives near–constant activation.

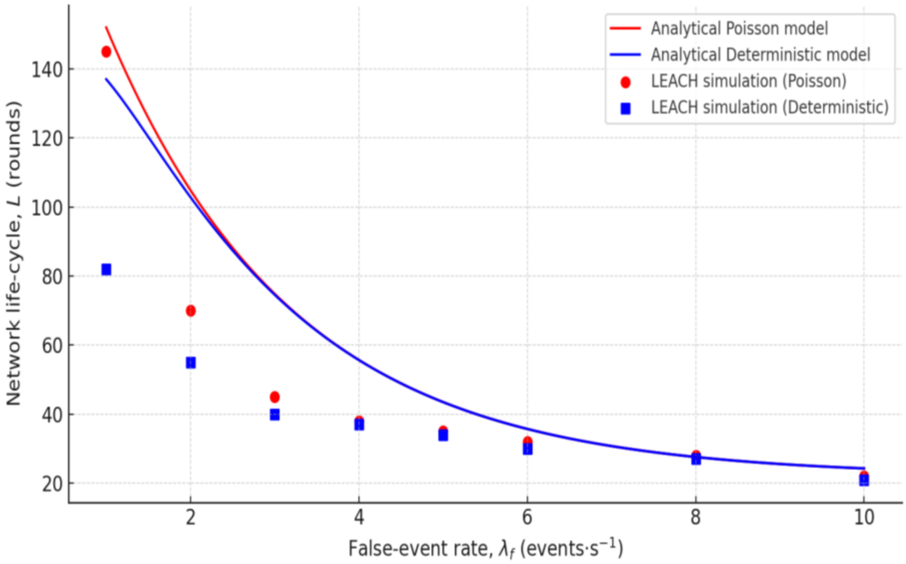

Fig. 2. Comparison of Poisson and deterministic induced false–event streams

At low intensities ($\lambda_f \leq 2$), the deterministic curve lies below the Poisson curve, implying a shorter life–cycle. The reason is structural: evenly spaced triggers keep radios active with fewer idle micro–intervals, so P_{loss} is more fully realised within each round. Poisson arrivals, by contrast, introduce random inter–arrival gaps that permit short sleep episodes or reduced contention, slightly extending L . As $\lambda_f \geq 4$, both curves converge (consistent with $\frac{dL}{d\lambda_f} \to 0$) because operation enters a steady regime dominated by continuous reporting where arrival regularity no longer changes the energy balance. This convergence aligns with prior traffic self–similarity observations in data networks [81, 85, 106] and with sensor–network energy studies [88, 89, 107], though our model explicitly accounts for mobility–induced re–clustering overhead.

In addition to the analytical trends, the LEACH simulation points included in Figure 2 empirically confirm the theoretical relationships. The discrete values follow the same trajectory as the analytical curves, with minor stochastic deviations attributable to random cluster–head rotation and dynamic channel contention. The agreement between the simulated and analytical results validates the correctness of the proposed energy model $E_{evt}(v)$ and its applicability to real clustered IoT topologies. Consequently, the combined depiction demonstrates not only the theoretical dependence of $L(\lambda_f)$ but also its physical observability within operational LEACH–based networks.

The final stage of the experimental analysis transfers the comparison from a purely descriptive level to a direct methodological contrast with reduced baseline schemes. This comparison is necessary because the analytical contribution of the proposed formulation consists not only in showing that induced false-event traffic degrades the network life-cycle, but also in providing a quantitatively more adequate estimate of this degradation. For that reason, the next figure presents the dependence $L(\lambda_f)$ not only for the proposed model, but also for two conventional approximations. The first approximation corresponds to the classical LEACH-style energy accounting and neglects the induced-loss term associated with false-event activation. The second approximation retains the traffic-rate effect, but treats it only as an average additional load and therefore does not reproduce the full coupling embedded in (3)–(5). Such a construction makes it possible to compare not only the direction of the trend, but also the closeness of each estimate to the LEACH simulation reference.

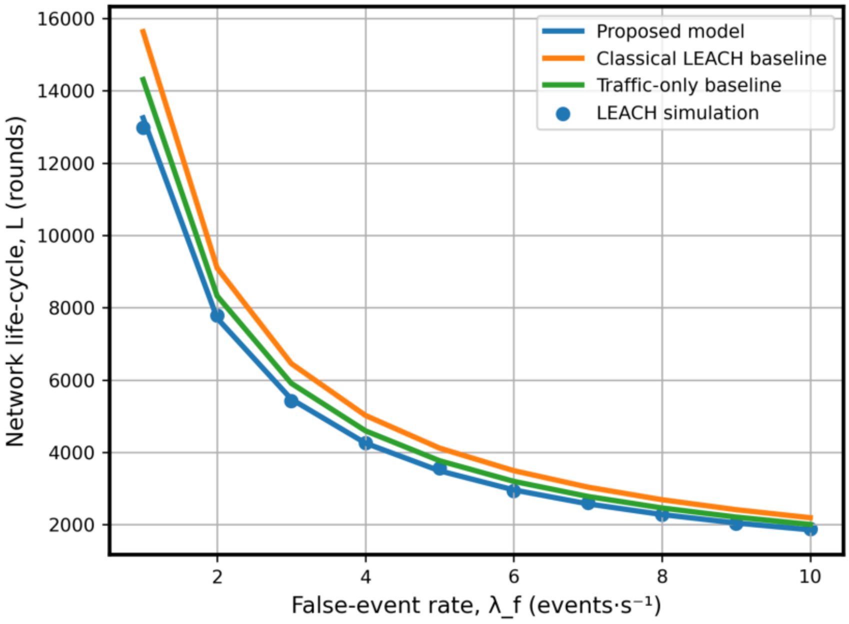

Fig. 3. Comparative network life-cycle estimates for the proposed model and reduced baselines

Figure 3 shows that all three analytical curves reproduce the same monotone decline of network life-cycle as the false-event rate increases, yet they differ substantially in quantitative adequacy. The most important divergence is observed already at the lower boundary of the interval. At $\lambda_f = 1$, the proposed estimate is close to 1.30×10^4 rounds and practically coincides with the simulation value, whereas the traffic-only and classical LEACH baselines overestimate the life-cycle at about 1.43×10^4 and 1.56×10^4 rounds, respectively. The same ranking is preserved in the middle of the interval: at $\lambda_f = 5$, the proposed model gives approximately 3.55×10^3 rounds against about 3.60×10^3 in simulation, while the traffic-only and classical LEACH baselines remain noticeably higher, at about 3.84×10^3 and 4.12×10^3 rounds. Even at the upper boundary, $\lambda_f = 10$, the proposed estimate stays close to the simulation reference, about 1.86×10^3 versus 1.88×10^3 rounds, whereas the two reduced schemes still overestimate the network life-cycle. Thus, Figure 3 demonstrates not only the general degradation trend, but also the stable quantitative advantage of the proposed formulation over the entire investigated range.

A visual comparison of lifetime curves, however, is still insufficient if the objective is to justify the claim of improved estimation accuracy in explicit quantitative terms. For this reason, the final figure reformulates the same comparison in error coordinates with respect to the LEACH simulation reference. The relative prediction error is used here because it directly measures the deviation between each analytical estimate and the corresponding simulation-based value. In the present context, this representation is methodologically stronger than a second qualitative comparison of $L\left(\lambda_f\right)$, since it makes the rank ordering of the competing approaches numerically explicit and shows whether the gain of the proposed formulation is stable across the whole interval of induced false-event rates.

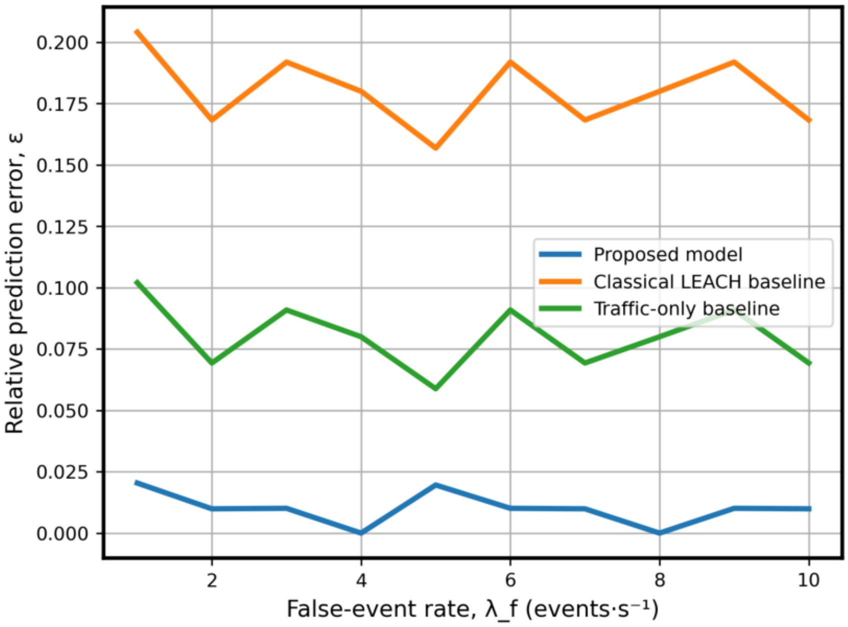

Fig. 4. Relative prediction error of the proposed model and reduced baselines with respect to LEACH simulation

Figure 4 confirms the result obtained in Figure 3 at a stricter quantitative level. The proposed model maintains the smallest prediction error throughout the full λ_f range and remains within approximately 0%–2%. This is most clearly seen at three representative points. At $\lambda_f = 1$, the error is about 2.0% for the proposed model, compared with approximately 10.2% for the traffic-only baseline and 20.4% for the classical LEACH baseline. At $\lambda_f = 5$, the proposed formulation still remains near 2.0%, whereas the traffic-only and classical LEACH baselines yield about 5.9% and 15.7%, respectively. At $\lambda_f = 10$, the proposed model preserves its advantage, with an error of about 1.0%, compared with about 6.9% for the traffic-only baseline and 16.8% for the classical LEACH baseline. These values show that the gain of the proposed model is systematic rather than local: compared with the traffic-only approximation, the prediction error is reduced several-fold, and compared with the classical LEACH baseline, by roughly an order of magnitude at the most sensitive points of the interval. Therefore, the revised comparison supports the claim that explicit incorporation of induced false-event losses provides a substantially more adequate estimate of network life-cycle.

Conclusions

This study has proposed an energy–aware analytical framework for modelling the life–cycle of an IoT network under induced false–event flows by integrating probabilistic traffic characteristics, communication–energy consumption, and network geometry. The obtained model establishes an explicit relationship between false–event arrival parameters and the temporal evolution of the network's energy resources.

It has been shown that the energy cost of a single false event acts as the fundamental mechanism driving large–scale network degradation. Extending this micro–level description to a network–wide energy balance yields a closed–form life–cycle expression that quantifies the impact of false–event arrival rate and node mobility on operational duration. A comparative analysis of Poisson and deterministic induced traffic demonstrates that arrival regularity significantly affects early–stage energy depletion, while both regimes converge to a saturation behaviour at high intensities.

Simulation results for a LEACH–based clustered IoT network confirm the analytical predictions and demonstrate that the proposed formulation provides a more accurate estimate of network life–cycle than reduced baseline approaches that consider only stationary energy consumption or average traffic load. In particular, the comparative analysis presented in the experimental section shows that the proposed model remains closest to the simulation reference across the entire range of induced false–event rates.

Future research may extend the framework to heterogeneous node energies, adaptive clustering, and time–varying false–event intensities, providing a basis for subsequent survivability– and availability–oriented analyses under induced influences.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

Conceptualization C.Y.; methodology C.Y.; validation C.Y.; formal analysis, V.K.; investigation, C.Y.; writing - original draft preparation, V.K.; writing - review and editing, C.Y.; visualization, C.Y., V.K.; project administration, V.K.

DECLARATION ON THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE TOOLS

In preparing this work, the author used Grammarly for: grammar and spelling checks. After using this tool/service, author reviewed and edited the content and take full responsibility for the content of this publication.

REFERENCES

1. Z. Almudayni, B. Soh, H. Samra, and A. Li, "Energy Inefficiency in IoT Networks: Causes, Impact, and a Strategic Framework for Sustainable Optimisation," Electronics, vol. 14, no. 1, p. 159, Jan. 2025, https://doi.org/10.3390/electronics14010159
2. S. O. Muhanji, A. E. Flint, and A. M. Farid, "The Development of IoT Within Energy Infrastructure," eIoT. Springer International Publishing, pp. 27–90, 2019. https://doi.org/10.1007/978-3-030-10427-6_3
3. Y. Huang, M. F. Antwi-Afari, B. Sun, and J. Liu, "Critical success factors for implementing self-powered wearable internet of things sensors in construction: A systematic literature review and conceptual framework," Applied Energy, vol. 401, p. 126836, Dec. 2025, https://doi.org/10.1016/j.apenergy.2025.126836
4. O. Popoola, M. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, and J. Popoola, "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, challenges and solutions," Blockchain: Research and Applications, vol. 5, no. 2, p. 100178, Jun. 2024, https://doi.org/10.1016/j.bcra.2023.100178
5. V. Merlino and D. Allegra, "Energy-based approach for attack detection in IoT devices: A survey," Internet of Things, vol. 27, p. 101306, Oct. 2024, https://doi.org/10.1016/j.iot.2024.101306
6. I. Das, R. N. Shaw, and S. Das, "Analysis of Energy Consumption of Energy Models in Wireless Sensor Networks," Lecture Notes in Electrical Engineering. Springer Singapore, pp. 755–764, Jul. 26, 2020. https://doi.org/10.1007/978-981-15-4692-1_57
7. C. Portillo, J. Martinez-Bauset, V. Pla, and V. Casares-Giner, "Energy Consumption Modeling for Heterogeneous Internet of Things Wireless Sensor Network Devices: Entire Modes and Operation Cycles Considerations," Telecom, vol. 5, no. 3, pp. 723–746, Aug. 2024, https://doi.org/10.3390/telecom5030036
8. E. A. Evangelakos, D. Kandris, D. Rountos, G. Tselikis, and E. Anastasiadis, "Energy Sustainability in Wireless Sensor Networks: An Analytical Survey," JLPEA, vol. 12, no. 4, p. 65, Dec. 2022, https://doi.org/10.3390/jlpea12040065
9. K. Boussaoud, A. En-Nouaary, and M. Ayache, "Adaptive Congestion Detection and Traffic Control in Software-Defined Networks via Data-Driven Multi-Agent Reinforcement Learning," Computers, vol. 14, no. 6, p. 236, Jun. 2025, https://doi.org/10.3390/computers14060236
10. S. Reno and K. Roy, "Navigating the Blockchain Trilemma: A Review of Recent Advances and Emerging Solutions in Decentralization, Security, and Scalability Optimization," CMC, vol. 84, no. 2,

pp. 2061–2119, 2025, https://doi.org/10.32604/cmc.2025.066366

11. M. S. Nkambule, A. N. Hasan, and T. Shongwe, "A review of intelligent control strategies for energy management systems in microgrids," Energy Conversion and Management: X, vol. 28, p. 101323, Oct. 2025, https://doi.org/10.1016/j.ecmx.2025.101323

12. M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open RAN security: Challenges and opportunities," Journal of Network and Computer Applications, vol. 214, p. 103621, May 2023, https://doi.org/10.1016/j.jnca.2023.103621

13. H. K. Armeniakos, P. S. Bithas, S. A. Tegos, A. G. Kanatas, and G. K. Karagiannidis, "Stochastic Geometry for Modeling and Analysis of Sensing and Communications: A Survey," IEEE Commun. Surv. Tutorials, vol. 28, pp. 2691–2724, 2026, https://doi.org/10.1109/comst.2025.3594560

14. J. Akshya et al., "Geometric Optimisation of Unmanned Aerial Vehicle Trajectories in Uncertain Environments," Vehicular Communications, vol. 54, p. 100938, Aug. 2025, https://doi.org/10.1016/j.vehcom.2025.100938

15. J. Chebil, H. Zormati, and J. B. Taher, "Geometry-Based Channel Modelling for Vehicle-to-Vehicle Communication: A Review," International Journal of Antennas and Propagation, vol. 2021, pp. 1–10, Aug. 2021, https://doi.org/10.1155/2021/4293266

Чень ЮЙ
Вінницький національний технічний університет
Гуансійський аграрний професійно-технічний університет
В'ячеслав КОВТУН
Вінницький національний технічний університет

ЕНЕРГООРІЄНТОВАНЕ МОДЕЛЮВАННЯ ЖИТТЄВОГО ЦИКЛУ IOT-МЕРЕЖІ ЗА УМОВ ІНДУКОВАНИХ ПОТОКІВ ХИБНИХ ПОДІЙ

У статті запропоновано енергоорієнтовану аналітичну модель життєвого циклу IoT-мережі за умов індукованого потоку хибних подій. У дослідженні розглядаються подієво-орієнтовані кластеризовані IoT-мережі, що функціонують під дією зовнішніх впливів, які генерують хибні повідомлення про події та спричиняють зайві операції сенсингу, передавання, приймання й ретрансляції даних. На відміну від традиційних підходів, які зазвичай розглядають поведінку трафіку, енергоспоживання комунікації та геометрію мережі окремо, запропонована модель інтегрує ці компоненти в єдиній формальній структурі. У межах цієї структури енергетичну вартість однієї хибної події формалізовано та пов'язано з енергетичним балансом мережі, параметрами надходження хибних подій і мобільністю вузлів. На цій основі отримано замкнені аналітичні вирази для опису часової еволюції залишкових енергетичних ресурсів і тривалості життєвого циклу мережі за фіксованої просторової топології. Модель установлює явний зв'язок між інтенсивністю індукованих хибних подій та виснаженням енергетичних ресурсів мережі. Показано, що інтенсивність і регулярність надходження хибних подій істотно впливають на траєкторію енергетичної деградації мережі. Зокрема, регулярніший індукований трафік змінює характер виснаження ресурсів на початкових етапах функціонування, тоді як за високих інтенсивностей різні режими трафіку збігаються до режиму насичення скорочення життєвого циклу мережі. Модель перевірено за допомогою моделювання для кластеризованої IoT-мережі на основі протоколу LEACH. Результати моделювання підтверджують аналітичні залежності в досліджуваному діапазоні 1 ≤ λ_f ≤ 10 та демонструють близьку відповідність запропонованої моделі до результатів симуляції. У порівняльному аналізі похибка прогнозування запропонованої моделі не перевищує приблизно 0%–2%, тоді як для моделі із середнім трафіковим навантаженням вона сягає близько 10,2%, а для класичної оцінки LEACH — близько 20,4%. Отримані результати свідчать, що запропонована модель забезпечує адекватнішу оцінку життєвого циклу мережі, оскільки явно враховує втрати енергії, індуковані хибними подіями, які в традиційних підходах ігноруються або суттєво спрощуються.

Ключові слова: IoT-мережі; хибні події; енергоорієнтоване моделювання; життєвий цикл мережі; ймовірнісний трафік; кластеризовані IoT-системи.