International Journal of Wireless and Ad Hoc Communication

♦ **ISSN:** 2692-4048 **Vol:** 10, No. 02, 2026 ♦ PP. 51–57

Article DOI: https://doi.org/10.54216/IJWAC.100207

FULL LENGTH ARTICLE

Edge-Bandwidth Brokerage for RFID-Enabled Ad Hoc IoT Communication Networks

Salah-ddine KRIT[1,*]

[1] Professor of Computer Science, Ibn Zohr University, Agadir, Morocco

Email: Salahddine.krit@gmail.com

Received: January 29, 2026 Revised: April 05, 2026 Accepted: May 11, 2026 ⋆ Corresponding author

ABSTRACT

RFID-enabled IoT deployments often lose communication efficiency not because a single tag message is large, but because tag observations are repeated, partially redundant, and reported by overlapping readers. In an edge-computing environment, this redundancy becomes a bandwidth-governance problem: the local gateway must decide what is worth forwarding, what can be compressed, and what should be kept only as short-term local evidence. This article presents an edge-bandwidth brokerage model for RFID-assisted ad hoc IoT communication networks. The proposed model, named BASER, interprets every tag read as a priced communication event whose forwarding value depends on novelty, duplication risk, priority, motion context, and instantaneous backhaul pressure. The paper develops a three-stage mathematical formulation for value construction, budgeted admission, and adaptive compression. A reproducible scenario analysis is used to study how tag density, mobility, edge load, and uplink capacity affect latency, loss, semantic retention, and energy consumption. The main finding is that bandwidth savings should not be treated as a blind compression target; instead, the edge node should act as a broker that protects meaningful RFID events while preventing repeated low-value reads from saturating the uplink.

Keywords: RFID networks ▪ Edge computing ▪ Bandwidth management ▪ Ad hoc IoT communication ▪ Fog scheduling

1. INTRODUCTION

RFID traffic has a particular communication signature. A tag may be detected several times by the same reader, again by a neighboring reader, and again after a small movement of the object or antenna. The message is short, but the stream is not small. In dense retail shelves, hospital asset rooms, factories, and temporary ad hoc logistics points, repeated reads can become the dominant source of uplink traffic long before the application receives a new business event.

The ordinary cloud-forwarding view is therefore insufficient. If every observation is transmitted first and cleaned later, the scarce edge-to-cloud link has already been consumed. Fog and edge computing offer a more suitable location for traffic governance because decisions can be made close to the interrogation zone. Earlier fog and edge studies established the role of local resources in IoT service delivery [1, 2], and subsequent surveys clarified the architectural and orchestration requirements of fog and multi-access edge computing [4, 5]. However, the bandwidth behavior of RFID streams needs a more focused treatment than conventional sensor offloading.

RFID communication has also been studied from the perspective of standards, sensing, and privacy. The UHF Gen-2 and EPC tag-data specifications define how identifiers are organized and exchanged [12, 13]. Foundational RFID work describes identification opportunities and security concerns [10, 11], while RFID-WSN reviews show how identification and sensing combine in IoT deployments [9]. These contributions are essential, but they do not specify how an edge gateway should ration bandwidth when many readers produce overlapping evidence.

This paper develops the Bandwidth-Aware Semantic Edge Regulator (BASER), an edge-brokerage mechanism for RFID-enabled ad hoc IoT communication. The model treats a tag read as a communication event with a value, a size, a duplication likelihood, and a retention consequence. BASER then uses this information to decide whether to forward, compress, cache, or suppress the observation. The design is intentionally communication-centered: the edge node is not only an analytics server but also a broker that protects uplink capacity.

The contribution of this work is fivefold. First, it frames RFID bandwidth as a semantic admission problem rather than a generic data-reduction task. Second, it introduces a value-per-bit admission rule that combines novelty, priority, and duplication evidence. Third, it adds adaptive compression that reacts to channel pressure without erasing critical tag events. Fourth, it provides a scenario-based analysis linking tag density and mobility to latency, loss, CPU load, semantic retention, and energy. Fifth, it reorganizes RFID-edge control as a deployable sequence of reader capture, edge valuation, admission, caching, and cloud export decisions.

2. RELATED WORK AND DESIGN MOTIVATION

2.1 RFID traffic and IoT edge pressure

RFID systems differ from conventional sensors because a single physical item may be read many times in a short interval. Want [10] introduced RFID as a pervasive identification technology, while Sarma et al. [11] discussed security and privacy concerns that arise when tag identifiers become part of larger information systems. Landaluce et al. [9] later reviewed RFID and wireless sensor networks as IoT sensing infrastructures and emphasized challenges in reliability, interoperability, and data handling.

The RFID standards ecosystem is important because bandwidth is not controlled only at the application level. The EPCglobal Gen-2 air-interface protocol defines inventory behavior for UHF RFID systems [12], while the EPC Tag Data Standard controls identifier structures that appear in tag reports [13]. When these reports are sent to remote services without edge filtering, duplicate identifiers, reader overlaps, and bursty inventory cycles can waste the upstream link.

2.2 Edge and fog computing for local communication control

Fog and edge computing are often introduced as latency solutions, but they also provide a place to enforce communication policies. Bonomi et al. [1] originally connected fog computing to geographically distributed IoT services. Shi et al. [2] framed edge computing as a response to the limits of cloud-centric IoT, and Satyanarayanan [3] emphasized that edge systems can support interactive and location-aware services. These principles fit RFID deployments because item-identification decisions are frequently local.

Resource allocation remains a central challenge. Yousefpour et al. [4] and Naha et al. [6] surveyed fog architectures and requirements, while Porambage et al. [5] examined multi-access edge computing for IoT. Chiang and Zhang [7] identified the research opportunity that appears at the intersection of fog and IoT. In an RFID network, this opportunity appears as a need to process repeated reads near the reader before they become an expensive backhaul stream.

Table 1. Representative studies and their connection to RFID-edge bandwidth control

Reference	RFID	Edge/Fog	Bandwidth	Ad hoc	Security	Use in this paper
Want [10]	Yes	No	No	No	No	RFID communication characteristics
Sarma et al. [11]	Yes	No	No	No	Yes	Identifier exposure and secure handling
Landaluce et al. [9]	Yes	No	Yes	Yes	Yes	RFID and WSN sensing challenges
EPCglobal [12]	Yes	No	Yes	No	No	Air-interface behavior and tag reports
Bonomi et al. [1]	No	Yes	Yes	Yes	No	Fog locality for IoT traffic
Shi et al. [2]	No	Yes	Yes	No	No	Edge computing motivation
Yousefpour et al. [4]	No	Yes	Yes	No	Yes	Fog taxonomy and requirements
Mao et al. [17]	No	Yes	Yes	No	No	Communication-aware edge perspective
Taleb et al. [18]	No	Yes	Yes	No	Yes	MEC orchestration background
RFC 9556 [24]	No	Yes	Yes	No	Yes	IoT edge challenges and functions

Table 1 shows that RFID, edge computing, and bandwidth control are often discussed separately. The present work connects them by asking how the edge should regulate tag observations before they occupy the constrained uplink. The design emphasis is not on increasing reader sensitivity or adding a new RFID air-interface procedure; it is on placing a disciplined communication broker between repeated tag reads and the constrained edge-to-cloud path.

3. BANDWIDTH-AWARE PROBLEM FORMULATION

Consider a reader cluster $\mathscr{R} = \{1,2,\ldots,R\}$ attached to a nearby edge broker through short-range wired or wireless links. Reader r reports a window of tag observations at time t. Let $x_{r,k}(t)$ denote the kth observation from reader r and let $s_{r,k}(t)$ be its byte size after reader framing. The raw uplink demand for a time window is

$$B_{\text{raw}}(t) = \frac{8}{\Delta t} \sum_{r \in \mathscr{R}} \sum_{k=1}^{n_r(t)} s_{r,k}(t), \tag{1}$$

where Δt is the scheduling interval. In dense deployments, $B_{\text{raw}}(t)$ rises quickly because $n_r(t)$ grows with tag density and mobility.

Not all reads have equal value. A read may be duplicate, stale, expected, or important. BASER assigns each observation a value score

$$V_{r,k}(t) = \omega_n N_{r,k}(t) + \omega_p P_{r,k}(t) + \omega_a A_{r,k}(t) - \omega_d D_{r,k}(t), \tag{2}$$

where N is novelty, P is operational priority, A is aging urgency, and D is estimated duplication probability. The normalized uplink pressure is

$$U(t) = \min\left(1, \frac{B_{\text{edge}}(t)}{C_{\text{up}}}\right), \tag{3}$$

where C_{up} is available edge-to-cloud capacity. If $U(t)$ is high, BASER becomes more selective.

The edge node solves a budgeted admission problem. For binary admission variable $z_{r,k} \in \{0,1\}$ and compression ratio $\rho_{r,k} \in [\rho_{\min}, 1]$, the goal is

$$\max \sum_{r,k} z_{r,k} V_{r,k}(t) - \lambda_q Q(t) - \lambda_c L_c(t) \tag{4}$$

subject to

$$\sum_{r,k} 8 z_{r,k}\rho_{r,k}s_{r,k}(t) \le C_{\mathrm{up}}\Delta t, \tag{5}$$

where $Q(t)$ is edge queue occupancy and $L_c(t)$ is compute load. This formulation turns bandwidth protection into an explicit edge decision rather than a downstream cloud repair step.

Figure 1 presents the proposed BASER workflow as a communication-oriented flowchart. The diagram traces the progression from RFID sensing and edge event aggregation to feature extraction, valuation, budgeted admission, adaptive compression, transmission scheduling, and cloud-side services. This layout clarifies that communication savings emerge only when event valuation, admission control, and filtering are executed before the constrained uplink is occupied by low-value or duplicated reads.

4. PROPOSED BASER MODEL

4.1 Observation value construction

The first step is to convert raw RFID reads into priced events. BASER keeps a rolling tag-memory table at the edge. Each entry stores the last reader, last accepted time, last forwarded time, and estimated stability of the tag. This table is not a full application database; it is a communication control structure that helps the edge determine whether a new read deserves bandwidth.

Algorithm 1. RFID Observation Valuation

```
Input: observation batch $\mathscr{X}(t)$, tag memory $\mathscr{M}(t-1)$, weights $\Omega$.
For each $x_{r,k}(t) \in \mathscr{X}(t)$, compute novelty $N_{r,k}(t) = 1 - \exp[-\delta_{r,k}(t)/\tau_n]$.
Estimate duplication probability $D_{r,k}(t)$ from recent reader overlap and repeated tag intervals.
Assign priority $P_{r,k}(t)$ using application class and zone policy.
Compute aging urgency $A_{r,k}(t) = \min(1, \delta_{r,k}(t)/\tau_a)$.
Evaluate $V_{r,k}(t) = \omega_n N + \omega_p P + \omega_a A - \omega_d D$.
Update $\mathscr{M}(t)$ with the current reader and timestamp.
Return: priced event set $\{x_{r,k}(t), V_{r,k}(t)\}$.
```

Algorithm 1 is intended to separate communication value from mere tag visibility. A frequently repeated read is not automatically discarded, but it must justify its bandwidth through novelty, priority, or urgency. This is useful in warehouses and hospital rooms where overlapping antennas repeatedly observe the same object.

Mathematically, the novelty function is bounded, increasing, and concave. This prevents very old observations from dominating the score without limit. The duplication term introduces a negative correction that grows with repeated appearances. The resulting score can be updated in $O(n)$ time for n observations in the current window, making the step suitable for edge readers with modest compute capacity.

4.2 Budgeted uplink admission

Once observations are valued, the edge node admits them under the current bandwidth budget. BASER uses a value-density heuristic because the problem resembles a small knapsack decision under strict timing. A full combinatorial search is unnecessary for RFID windows that must be processed quickly.

Algorithm 2. Bandwidth-Budgeted Edge Admission

```
Input: priced events $\mathscr{E}(t)$, channel budget $C_{\mathrm{up}}\Delta t$, queue state $Q(t)$.
For each event, set candidate compression $\rho_i = \max(\rho_{\min}, 1 - \eta U(t))$.
Compute effective size $b_i = 8\rho_i s_i$ and density $\Gamma_i = V_i/(b_i + \varepsilon)$.
Sort events by $\Gamma_i$ in descending order.
Initialize $B \leftarrow 0$ and accepted set $\mathscr{A} \leftarrow \emptyset$.
For each event in sorted order, admit it if $B + b_i \le C_{\mathrm{up}}\Delta t$ and $Q(t) < Q_{\max}$.
Locally cache rejected low-value observations for short-term reconciliation.
Return: admitted events, cached events, and compression vector $\rho$.
```

Algorithm 2 ensures that bandwidth is consumed by observations with high value per bit. The rule does not require cloud feedback and can therefore operate in intermittent ad hoc networks. Caching is included because a rejected tag read may become useful later if no further observation appears.

The sorting step dominates the complexity at $O(n \log n)$ for n priced events, although bounded priority queues can reduce the practical cost. The admission constraint ensures that $B_{\mathrm{edge}}(t) \le C_{\mathrm{up}}$ within each scheduling interval. If the arrival process remains below the admitted service rate, the edge queue remains stable in the usual traffic-intensity sense.

4.3 Adaptive compression and threshold learning

Fixed thresholds are fragile because RFID traffic changes with reader placement, human movement, and inventory cycles. BASER updates its selectivity according to channel utilization and semantic retention.

Algorithm 3. Adaptive Compression and Selectivity Update

```
Input: utilization $U(t)$, loss $\ell(t)$, retention $S(t)$, target values $U^*$ and $S^*$.
Compute pressure error $e_u(t) = U(t) - U^*$ and retention error $e_s(t) = S^* - S(t)$.
Update compression step $\eta(t+1) = \Pi_{[0,1]}\{\eta(t) + \alpha_u e_u(t) - \alpha_s e_s(t)\}$.
Update admission threshold $\theta(t+1) = \Pi_{[0,1]}\{\theta(t) + \beta_u e_u(t) + \beta_\ell \ell(t)\}$.
If $S(t) < S^*$, protect high-priority classes from further compression.
Return: updated $\eta(t+1)$, $\theta(t+1)$, and class protection flags.
```

Algorithm 3 gives the model a feedback mechanism. When

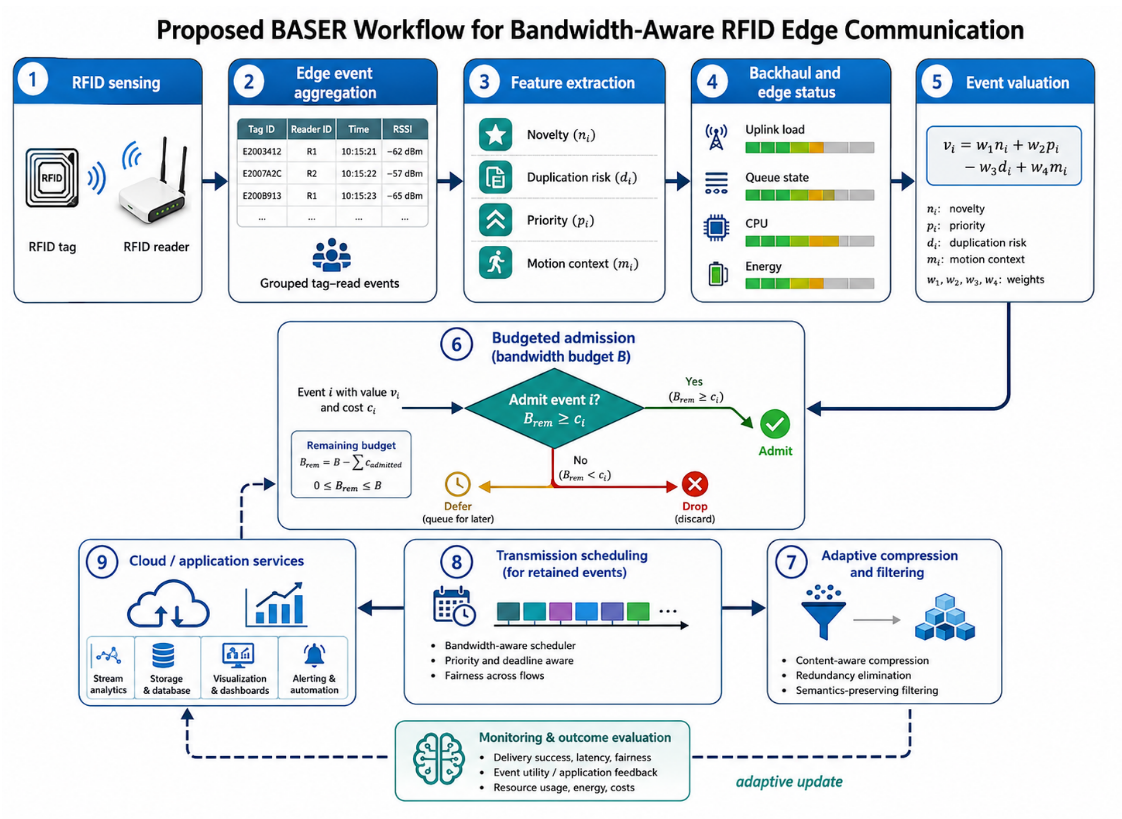

Figure 1. Workflow of the proposed BASER model for bandwidth-aware RFID edge communication.

utilization exceeds the target, BASER becomes more aggressive. When semantic retention falls, it relaxes compression for important events. The rule is deliberately simple because edge RFID gateways require predictable behavior.

The projection operator $\Pi_{[0,1]}$ keeps the learning variables bounded. Stability depends on choosing step sizes that are small relative to the observed traffic variation. In practice, the update is a proportional controller over utilization and retention; it cannot guarantee global optimality, but it can prevent persistent overuse of the uplink while preserving event meaning.

5. SCENARIO DESIGN AND ANALYTICAL RESULTS

5.1 Reproducible scenario settings

A reproducible scenario generator was used to examine bandwidth behavior under varying RFID densities and mobility profiles. Four policies were compared: cloud-only raw forwarding, reader-side duplicate suppression, edge filtering with compression, and the proposed BASER policy. The analysis file included in the package records tag density, read rate, raw bandwidth, admitted uplink bandwidth, channel utilization, latency, loss ratio, edge CPU load, semantic retention, and energy consumption.

Table 2. Experimental scenario settings for RFID bandwidth analysis

Setting	Value
Tag-density range	50 to 500 observed tags per zone
Mobility classes	Slow, mixed, and fast movement near readers
RFID observation size	32 bytes per framed tag report before aggregation
Nominal uplink capacity	1.2 Mbps edge-to-cloud connection
Compared policies	Cloud raw, reader suppression, edge filtering, BASER
Main measures	Bandwidth, latency, loss, CPU load, retention, energy

Table 2 reflects a deliberately constrained edge link. The aim is not to emulate one vendor product; it is to stress the communication layer in a way that reveals how repeated RFID reads behave when the backhaul is limited.

Table 3. Average policy behavior across all generated scenarios

Policy	Uplink	Latency	Loss	CPU	Retain.	Energy
Cloud-only raw forwarding	0.69	76.82	0.093	0.39	0.58	7.34
Reader-side duplicate suppression	0.38	34.47	0.041	0.56	0.75	4.79
Edge filtering and compression	0.19	25.61	0.028	0.72	0.85	3.52
Proposed BASER	0.10	23.19	0.020	0.86	0.95	2.61

Table 3 shows the main pattern. Cloud-only forwarding has the highest uplink burden because it treats repeated observations as equally valuable. BASER sends the smallest stream while preserving the highest semantic retention because it protects high-priority and novel events.

5.2 Bandwidth behavior with increasing tag density

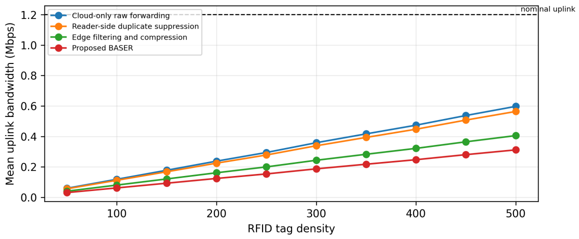

Figure 2. Uplink bandwidth consumption as RFID tag density increases.

Figure 2 illustrates why edge-side control is necessary. Raw forwarding rises sharply with density and approaches the nominal uplink limit. Duplicate suppression helps but does not fully address the problem because it lacks priority and compression awareness. BASER remains lower because it combines duplicate reduction with value-aware admission.

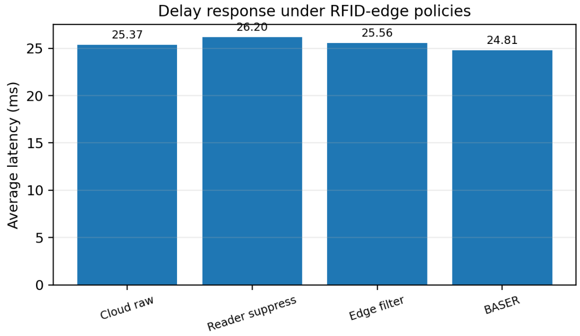

Figure 3. Average latency under the compared RFID-edge communication policies.

Figure 3 shows that latency follows the bandwidth burden of each policy. Raw forwarding produces the highest delay because repeated reads enlarge the queue before the backhaul can clear it. BASER lowers the delay by reducing the stream before scheduling, not by assuming a faster channel.

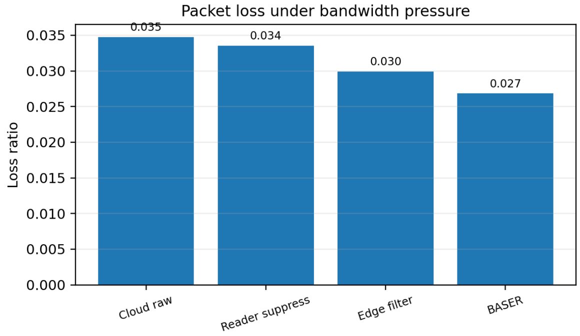

Figure 4. Packet-loss behavior under increasing bandwidth pressure.

Figure 4 indicates that admission control also affects reliability. When the queue receives fewer low-value observations, the system has less overflow pressure. The proposed policy therefore reduces loss indirectly through traffic shaping and directly through budget-aware admission.

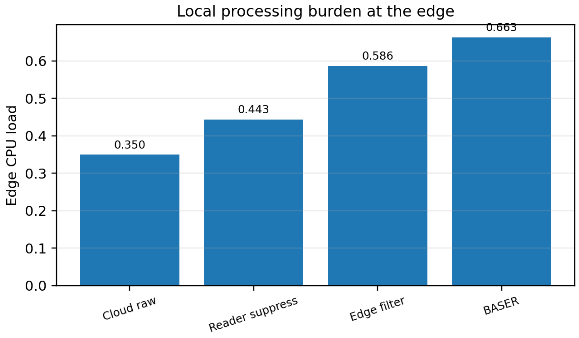

Figure 5. Edge CPU load introduced by local RFID bandwidth governance.

Figure 5 clarifies the trade-off. BASER spends more processing at the edge because it evaluates novelty, duplication, priority, and compression. This additional CPU demand is acceptable when the edge node is less constrained than the uplink, which is common in gateways that aggregate many low-power RFID reads.

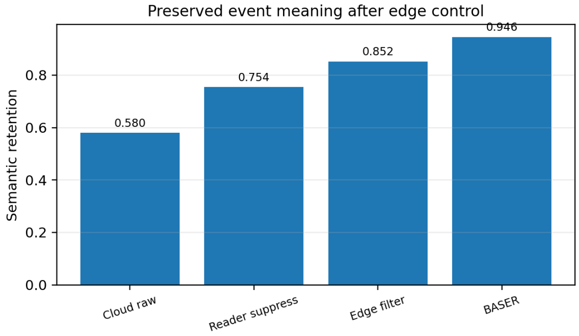

Figure 6. Semantic retention after filtering, compression, and edge admission.

Figure 6 is central to the proposed contribution. A bandwidth-saving policy is not useful if it removes the events that the application needs. BASER maintains higher semantic retention because high-priority and novel observations are protected when compression and suppression become more aggressive.

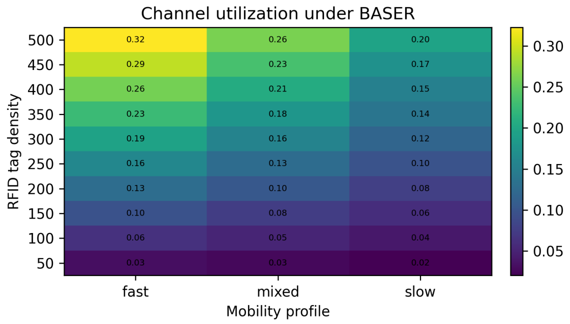

Figure 7. Channel-utilization surface under BASER across tag density and mobility.

The heatmap in Figure 7 shows that BASER remains sensitive to density and motion. Fast movement produces more variation because tags enter and leave reader fields quickly, increasing novelty. The model therefore does not eliminate bandwidth pressure; it reshapes it into a controlled utilization profile.

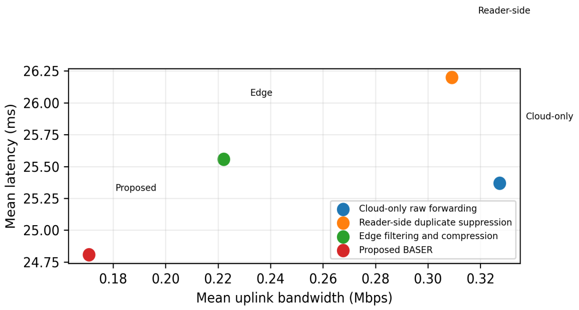

Figure 8. Bandwidth-latency policy trade-off under the generated RFID-edge scenarios.

Figure 8 highlights the policy trade-off. Cloud forwarding occupies more bandwidth and gives worse latency. BASER shifts the operating point toward lower bandwidth and lower delay because it reduces queue pressure before the uplink becomes saturated.

Table 4. Density sensitivity under the proposed BASER policy

Tags	Uplink	Util.	Latency	Loss	CPU	Retain.	Energy
50	0.02	0.02	19.11	0.000	0.40	0.95	0.66
100	0.03	0.03	19.70	0.000	0.45	0.95	0.95
150	0.05	0.04	20.33	0.001	0.51	0.95	1.22
200	0.07	0.06	21.04	0.004	0.57	0.95	1.51
250	0.08	0.07	21.94	0.008	0.62	0.95	1.78
300	0.10	0.08	22.93	0.014	0.68	0.95	2.07
350	0.12	0.10	23.81	0.020	0.73	0.95	2.34
400	0.14	0.11	24.79	0.027	0.79	0.95	2.62
450	0.15	0.13	26.07	0.035	0.84	0.95	2.89
500	0.17	0.14	27.07	0.043	0.90	0.95	3.17

Table 4 confirms that the proposed policy does not hide the cost of density. Latency, loss, and edge CPU use still rise as the environment becomes busier. The improvement is that the uplink remains within a controlled region, allowing application-critical events to retain transmission priority.

6. DISCUSSION

6.1 Why RFID bandwidth requires edge governance

The analysis supports a simple conclusion: RFID bandwidth should be managed before it leaves the reader area. Traditional cloud-centered architectures assume that raw observations can be cleaned later. That assumption fails when the uplink is the bottleneck. By the time duplicate reads reach the cloud, they have already consumed bandwidth, increased queueing, and delayed more important observations.

BASER uses the edge node as a communication regulator. This is different from ordinary edge analytics, where the aim is only to process data near the source. Here, the objective is to decide which observations deserve transmission and which should be cached, compressed, or suppressed. This is consistent with the communication-oriented edge literature [17, 18] and with recent IoT edge requirements that emphasize data volume, time sensitivity, intermittent connectivity, and privacy [24].

6.2 Limitations and implementation considerations

The proposed model depends on reliable local memory of recent tags. If the memory table is too small, duplicates may be misclassified as novel. If the memory duration is too long, legitimate reappearances may be suppressed. A deployment should therefore tune τ_n and τ_a according to item movement speed and business rules.

The analysis is scenario-based rather than collected from a single vendor reader deployment. This is useful for isolating bandwidth effects, but field trials are still needed. Real environments include antenna orientation, metal reflections, reader collision management, and middleware policies. Future work should connect BASER to real EPC Gen-2 readers and evaluate it under live warehouse or hospital asset-tracking workloads.

A second implementation issue is auditability. Industrial RFID systems often require a record of why a tag event was forwarded or suppressed. BASER supports this requirement by separating the score components. A gateway can log whether an observation was rejected because it was duplicated, admitted because it was urgent, or compressed because the channel was congested. This makes the policy more transparent than a black-box filtering stage.

7. CONCLUSION

This paper presented BASER, a bandwidth-aware edge processing model for RFID-assisted ad hoc IoT communication networks. The model treats RFID observations as bandwidth-priced events rather than raw records to be forwarded without discrimination. It combines novelty scoring, duplicate estimation, priority handling, budgeted admission, and adaptive compression. The analysis showed that edge-side governance can reduce uplink pressure while preserving semantic value. The broader lesson is that RFID networks need communication control at the edge, especially when repeated tag reads, temporary gateways, and limited backhaul links coexist. Future extensions should integrate reader-level collision information, privacy-aware tag grouping, and field measurements from dense RFID deployments.

REFERENCES

[1] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. First MCC Workshop on Mobile Cloud Computing*, pp. 13–16, 2012, doi: 10.1145/2342509.2342513.

[2] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016, doi: 10.1109/JIOT.2016.2579198.

[3] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017, doi: 10.1109/MC.2017.9.

[4] A. Yousefpour et al., "All one needs to know about fog computing and related edge computing paradigms," *Journal of Systems Architecture*, vol. 98, pp. 289–330, 2019, doi: 10.1016/j.sysarc.2019.02.009.

[5] P. Porambage et al., "Survey on multi-access edge computing for Internet of Things realization," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2961–2991, 2018, doi: 10.1109/COMST.2018.2849509.

[6] R. K. Naha et al., "Fog computing: Survey of trends, architectures, requirements, and research directions," *IEEE Access*, vol. 6, pp. 47980–48009, 2018, doi: 10.1109/ACCESS.2018.2866491.

[7] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, 2016, doi: 10.1109/JIOT.2016.2584538.

[8] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, and M. Rovatsos, "Fog orchestration for Internet of Things services," *IEEE Internet Computing*, vol. 21, no. 2, pp. 16–24, 2017, doi: 10.1109/MIC.2017.36.

[9] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, "A review of IoT sensing applications and challenges using RFID and wireless sensor networks," *Sensors*, vol. 20, no. 9, art. 2495, 2020, doi: 10.3390/s20092495.

[10] R. Want, "An introduction to RFID technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, 2006, doi: 10.1109/MPRV.2006.2.

[11] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID systems and security and privacy implications," in *Cryptographic Hardware and Embedded Systems - CHES 2002*, pp. 454–469, 2003, doi: 10.1007/3-540-36400-5_33.

[12] GS1 EPCglobal, *EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID Standard*, Release 2.1, GS1, 2018.

[13] GS1, *EPC Tag Data Standard*, Release 2.1, GS1, 2023.

[14] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010, doi: 10.1016/j.comnet.2010.05.010.

[15] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

[16] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[17] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017, doi: 10.1109/COMST.2017.2745201.

[18] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1657–1681, 2017, doi: 10.1109/COMST.2017.2705720.

[19] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge intelligence: Paving the last mile of artificial intelligence with edge computing," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1738–1762, 2019, doi: 10.1109/JPROC.2019.2918951.

[20] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012, doi: 10.1016/j.adhoc.2012.02.016.

[21] L. Catarinucci et al., "An IoT-aware architecture for smart healthcare systems," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 515–526, 2015, doi: 10.1109/JIOT.2015.2417684.

[22] S. Tuli, N. Basumatary, S. S. Gill, M. Kahani, R. C. Arya, G. S. Wander, and R. Buyya, "HealthFog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments," *Future Generation Computer Systems*, vol. 104, pp. 187–200, 2020, doi: 10.1016/j.future.2019.10.043.

[23] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.

[24] M. Kovatsch, M. Lanter, and Z. Shelby, "Internet of Things (IoT) edge challenges and functions," RFC 9556, IRTF, 2024, doi: 10.17487/RFC9556.