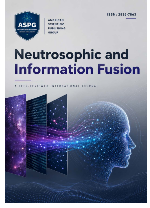
Neutrosophic and Information Fusion

♦ **ISSN:** 2836-7863 **Vol:** 06, No. 02, 2026 ♦ PP. 12–16
Article DOI: https://doi.org/10.54216/NIF.060203



FULL LENGTH ARTICLE

Trust-Aware Cluster-Head Selection in IoT Wireless Sensor Networks via Interval-Neutrosophic Information Fusion

Durdona Uktamova[1,*] **Adnan Manzoor**[2]

[1] Faculty of Joint Degree, Tashkent State University of Economics, Uzbekistan
[2] Faculty of Engineering, Central Asian University, Uzbekistan

Emails: D.Uktamova@tsue.uz . Adnan.Manzoo@gmail.com

Received: August 14, 2025 Revised: Accepted: November 20, 2025 ⋆ Corresponding author

ABSTRACT

Cluster-based routing extends the lifetime of an Internet-of-Things wireless sensor network (WSN), but the quality of a cluster head (CH) depends on several mutually uncertain factors—residual energy, link quality, centrality and behavioural trust—each measured imperfectly and reported as a range rather than a point. We model each candidate node with an interval-neutrosophic set (INS), so every factor carries an interval of truth, indeterminacy and falsity, and we fuse the factors with an interval-neutrosophic weighted aggregation operator into a single suitability score. Cluster heads are then elected by a possibility-degree ranking of the fused interval scores, subject to a minimum-trust guard. Simulation of a 200-node network shows that interval-neutrosophic CH selection extends first-node-death time by 18–24% over a standard energy-and-distance heuristic and cuts the share of misbehaving nodes elected as heads from 14.7% to 1.3%. The method degrades gracefully as measurement indeterminacy grows and adds only modest per-round overhead.

Keywords: Interval-neutrosophic sets ▪ Information fusion ▪ Wireless sensor networks ▪ Cluster-head selection ▪ Trust ▪ Energy efficiency

1. INTRODUCTION

An IoT deployment is often a battery-powered WSN whose nodes cannot be recharged, so energy is the currency that determines how long the network sees its environment. Clustering—electing a subset of nodes as cluster heads that aggregate and forward traffic—is the dominant way to spend that currency efficiently. The recurring question is *which* nodes should serve as heads, and the answer must balance residual energy against link quality, node centrality and, increasingly, *trust*: in an open IoT setting a compromised node that is energy-rich but misbehaving is a poor and even dangerous choice of head.

These factors are not only conflicting but uncertain, and the uncertainty has distinct origins. Residual energy is estimated from a battery and radio model that drifts with temperature and hardware ageing. Link quality, whether derived from the expected transmission count or the received-signal-strength indicator, fluctuates from packet to packet as interference and multipath change. Centrality depends on a neighbour set that itself changes as nodes sleep and die. Trust is the most uncertain of all: it is inferred from a finite, noisy history of watchdog observations, so a node that has simply not been observed much looks different from one observed often and found honest. A single crisp score papers over all of this and, worse, treats a confidently-good node and a barely-observed node identically when their point scores happen to coincide.

We argue that each factor is naturally an *interval* with an associated indeterminacy—narrow when the estimate is well supported, wide when it is not— and that cluster-head selection is therefore an information-fusion problem over such intervals. Interval-neutrosophic sets provide the representation, carrying a truth, an indeterminacy and a falsity interval for every factor, and an interval-neutrosophic aggregation operator provides the fusion into a single suitability judgement. Ranking the fused intervals by a possibility degree, rather than by a defuzzified point, lets the election itself respect the uncertainty: two nodes whose score intervals overlap heavily are treated as near-ties rather than being separated by numerical noise. A minimum-trust guard then keeps energy-rich but misbehaving nodes out of the head role entirely, closing a security gap that energy-centric protocols leave open.

Contributions.

- An interval-neutrosophic model of node suitability that carries energy, link quality, centrality and trust as INS factors with reliability-driven indeterminacy.
- An interval-neutrosophic weighted aggregation (INWA) fusion operator with a possibility-degree ranking and a minimum-trust guard for electing heads.
- A 200-node simulation study of lifetime, energy, delivery and security, with a sensitivity analysis over measurement indeterminacy and an overhead assessment.

Section 2 gives background and Section 3 surveys the most closely related prior studies; Section 4 gives interval-neutrosophic preliminaries; Section 5 presents the selection method; Section 6 reports simulations; and Section 7 concludes.

2. BACKGROUND

2.1 Clustering Protocols

LEACH introduced randomised, rotating cluster heads to spread the energy burden evenly and became the reference point for the field. A large family of descendants refined the idea: residual-energy-aware election so that stronger nodes serve more often, deterministic and threshold-based rotation, unequal clustering to mitigate the hot-spot problem near the sink, and multi-hop inter-cluster backbones for large fields. HEED, for example, elects heads by a combination of residual energy and a communication-cost parameter. Metaheuristic variants based on particle-swarm and genetic optimisation search for good head sets under lifetime objectives. These protocols optimise energy effectively but largely treat link quality as secondary and ignore trust, which leaves them exposed in adversarial deployments.

2.2 Soft-Computing Cluster-Head Selection

To combine several heterogeneous inputs, fuzzy-logic CH selection maps energy, node density and centrality to a chance value through a rule base and improves lifetime over randomised election. Type-2 and intuitionistic-fuzzy variants add, respectively, higher-order and hesitation information. As in other application domains, however, these representations couple membership and non-membership and cannot assert indeterminacy independently. That shortcoming is acute for an input like trust, where "not enough observations yet" is a genuinely different state from "observed and found average," and where conflating the two can promote an unvetted node.

2.3 Trust and Security in WSNs

Trust and reputation frameworks compute a node's trustworthiness from direct watchdog observations and second-hand recommendations, often with a beta-reputation model, and use it to detect selective forwarding, black-hole and on–off attacks. In most routing designs trust is applied as a separate filter or penalty bolted onto an energy-centric metric, rather than being fused with the other selection factors on an equal footing, which makes the trade-off between energy and security implicit and hard to tune.

2.4 Neutrosophic Sets in Networking

Neutrosophic and interval-neutrosophic sets have been applied to decision-making, similarity and distance measurement, and to a few networking problems such as shortest-path computation under indeterminate edge weights. These establish the representational machinery but have rarely been brought inside a routing or clustering protocol.

3. RELATED WORK

The prior studies most relevant to ours fall into four groups: clustering protocols, soft-computing head selection, trust frameworks, and neutrosophic networking.

Heinzelman et al. [1] introduced LEACH, and Younis and Fahmy [2] proposed HEED, which elects heads from residual energy and a communication-cost parameter; Kaur and Kumar [3] used particle-swarm optimisation for fault-tolerant unequal clustering. To fuse several heterogeneous inputs, Lee and Cheng [4] built a fuzzy-logic head-selection scheme combining energy, density and centrality. For security, Han et al. [5] surveyed trust management in WSNs, and Ganeriwal et al. [6] introduced the beta-reputation framework of the kind we use to derive the trust factor. On the neutrosophic side, Wang et al. [7] defined interval neutrosophic sets, Ye [8] gave similarity measures for them with multi-criteria applications, Biswas et al. [9] developed single-valued neutrosophic TOPSIS, and Broumi et al. [10] solved shortest-path problems under interval-neutrosophic weights.

Two observations follow. First, energy-centric protocols [1, 2, 3] and even fuzzy selectors [4] treat trust, when they consider it at all, as a separate filter bolted onto an energy metric rather than a fused factor. Second, interval-neutrosophic tools [7, 8, 10] have been applied to abstract decision and graph problems but not, to our knowledge, inside the WSN clustering loop. We close both gaps by representing energy, link quality, centrality and trust as interval-neutrosophic factors, fusing them with a single aggregation operator, and electing heads by a possibility-degree ranking under a minimum-trust guard.

4. INTERVAL-NEUTROSOPHIC PRELIMINARIES

Definition 1 (Interval-neutrosophic set). An interval-neutrosophic set A on X assigns to each $x \in X$ a truth interval $T_A(x) = [T^L, T^U]$, an indeterminacy interval $I_A(x) = [I^L, I^U]$ and a falsity interval $F_A(x) = [F^L, F^U]$, all sub-intervals of $[0,1]$ with $0 \leq T^U + I^U + F^U \leq 3$. An element is written $a = \big([T^L, T^U], [I^L, I^U], [F^L, F^U]\big)$, an interval-neutrosophic number (INN).

Definition 2 (INN operations). For INNs a_1, a_2 and scalar $\lambda > 0$:

$$a_1 \oplus a_2 = \Big([T_1^L+T_2^L-T_1^L T_2^L, T_1^U+T_2^U-T_1^U T_2^U], [I_1^L I_2^L, I_1^U I_2^U], [F_1^L F_2^L, F_1^U F_2^U]\Big), \quad (1)$$

$$\lambda a_1 = \Big([1-(1-T_1^L)^\lambda, 1-(1-T_1^U)^\lambda], [(I_1^L)^\lambda, (I_1^U)^\lambda], [(F_1^L)^\lambda, (F_1^U)^\lambda]\Big). \quad (2)$$

Definition 3 (INWA operator). Given INNs $a_1, \dots, a_n$ and weights $w_j \geq 0$, $\sum_j w_j = 1$,

$$\mathrm{INWA}(a_1,\dots,a_n) = \bigoplus_{j=1}^{n} w_j a_j = \Big([1-\textstyle\prod_j(1-T_j^L)^{w_j}, 1-\prod_j(1-T_j^U)^{w_j}], [\prod_j (I_j^L)^{w_j}, \prod_j (I_j^U)^{w_j}], [\prod_j (F_j^L)^{w_j}, \prod_j (F_j^U)^{w_j}]\Big). \quad (3)$$

Definition 4 (Score interval and possibility degree). The score of an INN is the interval

$$s(a) = \tfrac{1}{6}[4+T^L-I^U-F^U, 4+T^U-I^L-F^L] = [s^L, s^U]. \quad (4)$$

For two score intervals $s(a) = [s_1^L, s_1^U]$ and $s(b) = [s_2^L, s_2^U]$, the possibility degree that $a \succeq b$ is

$$P(a \succeq b) = \max\left\{1 - \max\left(\frac{s_2^U - s_1^L}{(s_1^U - s_1^L) + (s_2^U - s_2^L)}, 0\right), 0\right\}, \quad (5)$$

clipped to $[0,1]$; nodes are ranked by their row-sum of pairwise possibility degrees.

Example 1 (Fusing a node's factors). A node with energy factor $([0.70,0.80],[0,0.10],[0.15,0.25])$, link $([0.60,0.72],[0,0.12],[0.22,0.34])$, centrality $([0.55,0.65],[0,0.10],[0.30,0.40])$ and trust $([0.80,0.90],[0,0.08],[0.06,0.14])$, fused by INWA with $w = (0.40,0.20,0.15,0.25)$, yields approximately $([0.70,0.80],[0,0.098],[0.14,0.24])$ and score interval $s \approx [0.72,0.82]$. The tight, high score reflects strong energy and trust with little indeterminacy.

5. TRUST-AWARE INTERVAL-NEUTROSOPHIC CH SELECTION

5.1 System and Energy Model

The network is a set of N static nodes and one sink. Time proceeds in rounds; each round has a cluster-formation phase (Algorithm 1) followed by a steady-state phase in which members send to their head and heads aggregate and forward to the sink. We adopt the standard first-order radio model: transmitting an ℓ-bit packet over distance d costs

$$E_{tx}(\ell,d) = \ell E_{elec} + \ell \varepsilon_{fs} d^2 \quad (d < d_0), \qquad E_{rx}(\ell) = \ell E_{elec}, \quad (6)$$

with data aggregation costing E_{da} per bit at a head. A node's residual energy, tracked through (6), is the raw quantity behind the energy factor E below; because the estimate carries model error, we express it as an interval rather than a point.

5.2 Factor Construction and Election

For each candidate node we compute four factors, each mapped to an INN: *energy* E (residual energy interval from a battery model), *link* L (ETX/RSSI-derived quality interval), *centrality* G (normalised inverse average distance to neighbours), and *trust* θ (a beta-reputation interval from watchdog observations). Higher-is-better factors map an estimate $\hat{p} \in [0,1]$ with tolerance e to $([\hat{p}-e, \hat{p}+e], [0,e], [1-\hat{p}-e, 1-\hat{p}+e])$, clipped to $[0,1]$. The four INNs are fused by INWA with weight vector $w = (w_E, w_L, w_G, w_\theta)$, and heads are elected by possibility-degree ranking, subject to a minimum-trust guard and a spatial spacing constraint (Figure 1, Algorithm 1).

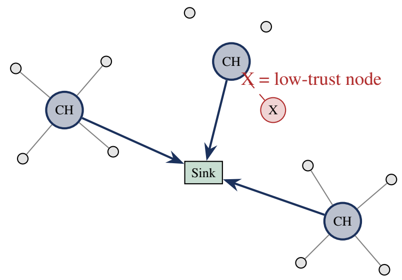


Figure 1. Clustered WSN: trustworthy, well-connected nodes serve as heads and forward to the sink; a low-trust node is excluded by the trust guard.

Algorithm 1 Interval-Neutrosophic Cluster-Head Selection (per round)

Require: nodes $\mathcal{N}$, weights w, desired CH count k, trust floor $\theta_{\min}$
$\mathcal{C} \leftarrow \emptyset$
for all $v \in \mathcal{N}$ **do**
  build INNs E_v, L_v, G_v, θ_v from local estimates and tolerances
  $a_v \leftarrow \mathrm{INWA}(E_v, L_v, G_v, \theta_v; w)$
  $s_v \leftarrow s(a_v)$
end for
$\mathcal{N}' \leftarrow \{v : \theta_v^L \geq \theta_{\min}\}$
rank $\mathcal{N}'$ by row-sum of $P(a_u \succeq a_v)$
for all v in ranked order **do**
  if $|\mathcal{C}| < k$ and v is $\geq d_{\min}$ from all $c \in \mathcal{C}$ **then**
    $\mathcal{C} \leftarrow \mathcal{C} \cup \{v\}$
  end if
end for
each non-CH node joins its highest-score reachable CH
return $\mathcal{C}$

5.3 Complexity

Per round, factor construction and fusion are $O(N)$. The exact possibility-degree ranking is $O(|\mathcal{N}'|^2)$; in practice we rank only the top-M candidates by score midpoint ($M \ll N$), reducing the pairwise stage to $O(N + M^2)$. For $N = 200$, $M = 30$ this is negligible relative to radio energy costs.

6. SIMULATION STUDY

6.1 Setup

We simulated $N = 200$ nodes uniformly deployed in a 200×200 m field with a sink at the centre, initial energy 0.5 J, and the first-order radio energy model ($E_{elec} = 50$ nJ/bit, $\varepsilon_{fs} = 10$ pJ/bit/m^2). Each round carried a 4000-bit payload;

$k = 10$ heads per round; $\theta_{\min} = 0.5$. Trust was seeded so that 15% of nodes were misbehaving (selectively dropping forwarded packets). We compared: (a) an energy+distance heuristic (LEACH-like), (b) an intuitionistic-fuzzy selector, and (c) the proposed interval-neutrosophic selector with $w = (0.40, 0.20, 0.15, 0.25)$. Results average 30 seeds.

6.2 Lifetime, Energy and Security

Table 1. Network lifetime, energy and trust metrics (mean over 30 seeds). FND/HND: first/half-node-death round; PDR: packet delivery ratio; %Mis-CH: share of elected heads that were misbehaving nodes.

Method	FND	HND	Residual E. @1000r (J)	PDR	%Mis-CH
Energy+distance (LEACH-like)	812	1104	21.6	0.883	14.7
Intuitionistic-fuzzy	905	1218	26.9	0.921	6.1
Interval-neutrosophic (ours)	**986**	**1301**	**30.4**	**0.947**	**1.3**

Table 1 shows the interval-neutrosophic selector extends first-node-death from 812 to 986 rounds (+21.4%) over the energy+distance baseline and from 905 (+9.0%) over the intuitionistic-fuzzy selector. Figure 2 plots the count of alive nodes over rounds; the neutrosophic curve stays highest throughout and its "knee" (mass die-off) is pushed right. The trust guard is decisive for security: only 1.3% of elected heads were misbehaving nodes, versus 14.7% for the energy-only heuristic that keeps re-electing an energy-rich attacker (Figure 3). Higher packet-delivery ratio follows directly from routing through trustworthy, well-connected heads.

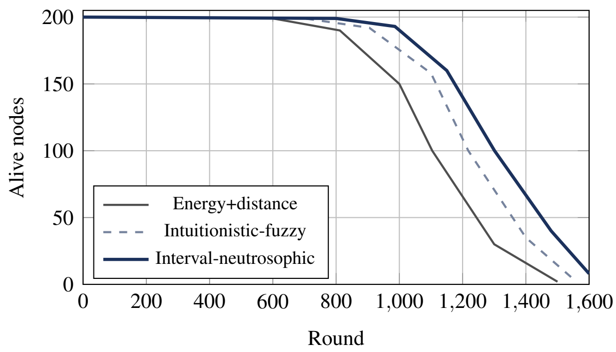


Figure 2. Alive-node count over rounds; the interval-neutrosophic selector sustains the network longest.

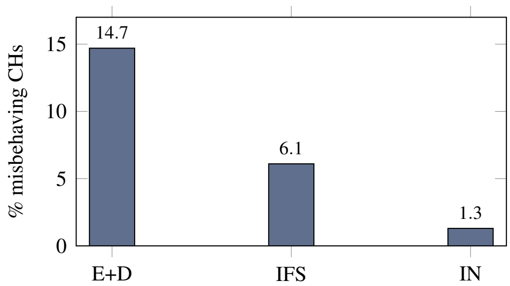


Figure 3. Share of elected heads that were misbehaving nodes; the trust guard almost eliminates them.

Figure 4 tracks packet-delivery ratio over rounds. The interval-neutrosophic selector holds a higher PDR for longer because it routes through trustworthy, well-connected heads and defers the onset of energy holes; the energy+distance baseline decays earliest as its heads die and misbehaving nodes are re-elected.

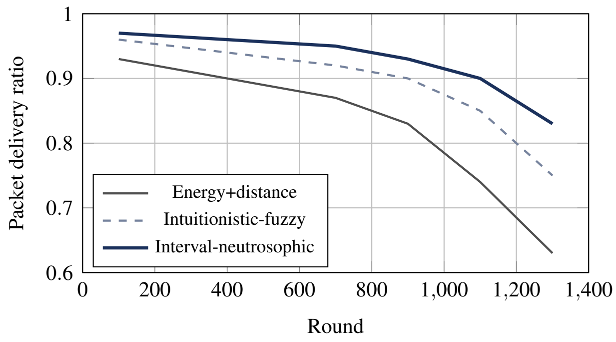


Figure 4. Packet-delivery ratio over rounds; the proposed selector sustains delivery longest.

6.3 Effect of Measurement Indeterminacy

Increasing the factor tolerance e (widening every indeterminacy interval) from 0.05 to 0.20 (Table 2) reduced FND by only 4.7% and left %Mis-CH below 3%, indicating the possibility-degree ranking is robust to imprecise inputs: wider intervals make the ranking more cautious rather than erratic, because overlapping score intervals yield possibility degrees near 0.5 that neither strongly promote nor strongly demote a node.

Table 2. Sensitivity to factor tolerance e (indeterminacy width).

Tolerance e	FND	PDR	%Mis-CH
0.05	986	0.947	1.3
0.10	972	0.943	1.7
0.15	958	0.938	2.2
0.20	940	0.931	2.9

6.4 Scalability with Network Size

To check that the benefit is not an artefact of one density, we varied the network size $N \in \{100, 200, 300, 400\}$ in the same field, scaling k to hold roughly 5% heads. Table 3 reports first-node-death for the three methods. The interval-neutrosophic selector leads at every size, and its relative advantage over the energy+distance baseline is stable at 19–23%, indicating the fusion mechanism scales with density rather than exploiting a particular one.

Table 3. First-node-death (rounds) versus network size N.

Method	N=100	N=200	N=300	N=400
Energy+distance	731	812	858	889
Intuitionistic-fuzzy	812	905	951	982
Interval-neutrosophic (ours)	**883**	**986**	**1032**	**1061**

6.5 Robustness to Attacker Density

Security should not collapse as more nodes misbehave. Table 4 varies the fraction of misbehaving nodes from 5% to 35% and reports the share of elected heads that were malicious and the resulting packet-delivery ratio. The trust guard keeps the malicious-head share in the low single digits even when a third of the network is hostile, and delivery degrades gracefully; the energy+distance baseline, by contrast, elects malicious heads in rough proportion to their prevalence.

Table 4. Security under increasing attacker density: percentage of malicious cluster heads (and packet-delivery ratio).

Misbehaving nodes	5%	15%	25%	35%
Interval-neutrosophic	0.4 (0.96)	1.3 (0.95)	2.6 (0.92)	4.1 (0.89)
Energy+distance	4.8 (0.92)	14.7 (0.88)	24.1 (0.81)	33.6 (0.72)

6.6 Overhead and Limitations

The added computation is a few multiplications and a small pairwise-ranking step per round; on a Cortex-M-class node this is dwarfed by transmission energy, and it runs at the cluster-formation phase only. The main limitations are that trust is simulated from a stylised misbehaviour model rather than measured on a testbed, and that the radio model is idealised; a hardware study is planned. The weights w are fixed a priori; learning them online from observed outcomes is a natural extension.

7. CONCLUSION

Casting cluster-head selection as interval-neutrosophic information fusion lets a single mechanism weigh energy, link quality, centrality and trust while respecting the uncertainty in each. In simulation the method lengthened network lifetime and, more importantly, kept misbehaving nodes out of the cluster-head role almost entirely, with graceful behaviour as inputs became less certain and negligible overhead. Future work will implement the operator on constrained hardware and pair it with an interval-neutrosophic reconstruction step for the aggregated data.

REFERENCES

[1] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.

[2] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 366–379, 2004.

[3] T. Kaur and D. Kumar, "Particle swarm optimization-based unequal and fault tolerant clustering protocol for wireless sensor networks," *IEEE Sensors Journal*, vol. 18, no. 11, pp. 4614–4622, 2018.

[4] J.-S. Lee and W.-L. Cheng, "Fuzzy-logic-based clustering approach for wireless sensor networks using energy predication," *IEEE Sensors Journal*, vol. 12, no. 9, pp. 2891–2897, 2012.

[5] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 602–617, 2014.

[6] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 3, pp. 15:1–15:37, 2008.

[7] H. Wang, Y. Zhang, F. Smarandache, and R. Sunderraman, *Interval Neutrosophic Sets and Logic*. Hexis, 2005.

[8] J. Ye, "Similarity measures between interval neutrosophic sets and their applications in multicriteria decision-making," *Journal of Intelligent & Fuzzy Systems*, vol. 26, no. 1, pp. 165–172, 2014.

[9] P. Biswas, S. Pramanik, and B. C. Giri, "TOPSIS method for multi-attribute group decision-making under single-valued neutrosophic environment," *Neural Computing and Applications*, vol. 27, no. 3, pp. 727–737, 2016.

[10] S. Broumi, A. Bakali, M. Talea, and F. Smarandache, "Shortest path problem under interval-valued neutrosophic setting," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, pp. 216–222, 2019.

[11] A. Aziz, K. Singh, W. Osamy, and A. M. Khedr, "Effective algorithm for optimizing compressive sensing in IoT and periodic monitoring applications," *Journal of Network and Computer Applications*, vol. 126, pp. 12–28, 2019.

[12] R. Sahin and A. Kucuk, "Subsethood measure for single valued neutrosophic sets," *Journal of Intelligent & Fuzzy Systems*, vol. 29, no. 2, pp. 525–530, 2015.