FMDB *Transactions on Sustainable Computing Systems*

Integrating Adaptive Trust-Driven Metaheuristic Clustering with Energy-Aware Decision Intelligence for Resilient Wireless Sensor Networks

Amsaveni Manigandan[1,*], M. Saranya[2]

[1,2]Department of Computer Science, P. K. R Arts College for Women, Gobichettipalayam, Tamil Nadu, India.
amsaveni.confident@gmail.com[1], drmsaranyamcapersonal@gmail.com[2]

Abstract: Wireless Sensor Networks (WSNs) play a fundamental role in contemporary data-centric applications, but are severely energy-limited and vulnerable to highly sophisticated insider attacks. Current protocols tend either to treat network lifetime and security as separate concerns (resulting in brittle and short-lived networks) or not consider the problem at all. This paper proposes a new integrated framework: The Adaptive Trust-Driven Metaheuristic Clustering with Energy-Aware Decision Intelligence (ATDMC-EADI). This architecture employs a multi-metric, adaptive trust-based model to dynamically monitor node behaviour, detecting malicious behaviours, including grey hole and black hole attacks. This trust factor, along with the remaining energy, is directly applied to a hybrid metaheuristic clustering algorithm for selecting resilient and high-energy cluster heads. This secure topology is then controlled by a high-level decision intelligence layer, which optimizes routing paths and sleep schedules. The ATDMC-EADI model is validated in the NS-3 (Network Simulator 3) environment using new data. We adopted a custom-created dataset, WSN-TrustSim-498, which contains 498 different network operating scenarios under multiple attack settings. The findings indicate that our integrated mechanism significantly outperforms baseline methods in terms of network lifetime, data correctness, and resilience against diverse insider threats.

Keywords: Wireless Sensor Networks (WSN); Network Resilience; Adaptive Trust; Metaheuristic Clustering; Energy-Aware; Decision Intelligence; Adversarial Conditions; Trust Models.

Received on: 24/10/2024, **Revised on:** 18/01/2025, **Accepted on:** 20/02/2025, **Published on:** 07/09/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCS

DOI: https://doi.org/10.69888/FTSCS.2025.000474

Cite as: A. Manigandan and M. Saranya, "Integrating Adaptive Trust-Driven Metaheuristic Clustering with Energy-Aware Decision Intelligence for Resilient Wireless Sensor Networks," *FMDB Transactions on Sustainable Computing Systems*, vol. 3, no. 3, pp. 157–165, 2025.

1. Introduction

Wireless Sensor Networks (WSNs) have emerged as a pervasive, data-driven technology for low-cost and large-scale in-situ sensing, as summarised by seminal surveys on WSN architectures [7]. They are used in various applications, such as environmental monitoring, industry automation, military surveillance, and healthcare, to gain real-time knowledge of physical systems. This is evident in some of the experiments presented in Sahoo et al. [1], which demonstrate real-world situations. However, such networks face several fundamental challenges; one of the most critical ones is the limited energy supply for

[*] Corresponding author.

many battery-powered nodes, which arguably preempts how long a network can function, as noted, for example, by lifetime prediction models in Al-Kaseem et al. [11]. In addition, insider attacks (e.g., black hole, grey hole, and sinkhole) make the secure deployment problem even more challenging, a phenomenon also studied in threat taxonomies, such as those by Nandan et al. [4]. To cope with the burden and address energy constraints, cluster-based protocols are superior techniques for nodes to aggregate data and send it to the elected cluster heads, as suggested in the Hierarchical Energy model by Sharma and Gupta [13]. Nonetheless, CH selection is a multi-objective problem. It has been traditionally addressed with metaheuristic optimisation-based nature-inspired algorithms—such as the anthill colony, the secretary bird, or albatross foraging—which have been applied to Intelligent Routing designs tested by Zhang et al. [6]. Nevertheless, energy-based remedies were ineffective in adversarial conditions because a single high-energy node can still be infected and spread throughout the network, as demonstrated in Al-Otaibi et al. [10] during security break role-playing game exercises.

At the other extreme, trust-based systems expend resources to monitor node behaviour, triggering false alarms for malicious operations, and incur a certain level of trade-off between the falseness of alarm triggers and energy efficiency by isolating nodes, as discussed in Kumar et al. [2]. While attempts have been made to combine energy-aware heuristics with trust models, these approaches have been hybrids, and for the most part, they have focused on security or optimisation. This is due to a lack of cooperation protocols, which lead to unstable and incident solutions, see, for instance, the comparative evaluation in Senthil et al. [3]. This lack drives the pursuit for a new model in which trust and energy can be considered inherent node selection and network maintenance co-evolving properties. It is claimed in Hsiao [12] that an integrated search of the clustering reviews similarly reflected this call.

To address this need, this paper introduces the ATDMC-EADI model, which combines an adversarial-aware approach with efficient energy consumption, as envisioned conceptually under the design of secure clustering by Fu et al. [5]. Because it consists of a 3-layer design with dynamic trustful evaluation, hybrid metaheuristic CH selection, and high decision intelligence, this framework has the objective to achieve longer lifetime and better resilience in WSN deployments in hostile and resource-restricted areas, as envisioned by recent robust networking schemes in Wang et al. [8], and experimentally confirmed by optimisation-enhanced security models handled in Gholami and Hamidzadeh [9].

2. Review of Literature

Over the years, the development of WSN protocols has been characterised by two fundamental and interdependent challenges that have emerged from seminal thoughts on energy neutrality, such as the founding models proposed by Nandan et al. [4], including fault tolerance and energy efficiency. The first two strategies, direct broadcasting and flooding, had both experienced significant signalling overhead. Therefore, cluster-based protocols were proposed to minimise long-range communications via hierarchical data aggregation, for example, the LEACH style proposed by Gholami and Hamidzadeh [9]. This paradigm shift led to a particular emphasis on CH selection, and probabilistic or deterministic approaches appeared to be less robust under dynamic scenarios, as shown in simulation studies published in Sahoo et al. [1]. Therefore, metaheuristic algorithms have become indispensable and are employed using nature-based approaches, including particle swarm optimisation (PSO), ant colony foraging, and simulated annealing, to find the optimal CH locations.

The latter techniques are integrated into energy-conscious clustering schemes, proposed by Zhang et al. [7]. Although most of these schemes significantly improved the network lifetime, they were based on ideal cooperation, which became impractical as insider threats, such as Black Hole and Sink Hole attacks, began to flourish. These hijacking, routing, and interrupted data flow are demonstrated through attack case studies provided in Hsiao [12]. These threats led to the development of security models based on trust. They monitored the behavior of nodes over time and computed reliability based on decentralized reputation monitoring mechanisms as formally defined by Fu et al. [5]. These models could contain malicious nodes that not only isolate them but also do not consider the overhead generated due to isolation and reclustering. This ineffectiveness has been exposed in trust-energy tradeoff analyses pooled in Senthil et al. [3]. To combat this siloed strategy, a new generation of hybrid techniques was developed, focusing on integrating metaheuristics to enhance efficiency.

Instead, the majority used a two-step approach in which security and energy were treated separately, with only trusted nodes being filtered, followed by an optimisation operator. This approach also has a drawback compared to protocol works, such as those by Al-Otaibi et al. [10]. Another essential missing bottleneck was the lack of a decision intelligence layer to manage topology after clustering, such as reorganising sleep schedules and routing paths. This requirement was met in adaptive optimisation systems proposed by Sharma and Gupta [13]. In summary, this literature emphasises the need for an integrated architecture that incorporates trust and energy as central dimensions of cluster cardinality fitness, facilitated through intelligence layers. This tendency is also prompted by robust WSN research works, such as Kumar et al. [2], and cross-domain optimisation methods proven in eco-secure routing algorithms [11]. Additionally, it has a bioadaptive inclination, as analysed in the swarm algorithm introduced in Zhang et al. [6].

3. Methodology

The multi-layered topological model proposed for the ATDMC-EADI architecture aims to provide an autonomous and reliable sensor network. It employs three combined stages: adaptive trust computation, metaheuristics-based clustering, and energy-aware decision intelligence. The first phase, the ATM, is executed in a decentralized and on-the-fly manner at each sensor. Every node serves as a watchdog, observing its own neighbours to monitor three key aspects of their local behaviour. The first factor, Packet Forwarding Integrity, measures the reliability of a neighbour's packet forwarding to ensure timely arrival, which helps identify black hole and grey hole behaviour. The second parameter, DCR, detects the presence of data falsification attacks between a node's sensor readings and previous data and averages. The third, Communication Overhead, aims to mitigate flooding attacks by discouraging nodes from sending excessive messages. Combined, these steps ensure that the sensor network adjusts to evolving conditions and threats while also remaining secure, efficient, and self-maintaining.

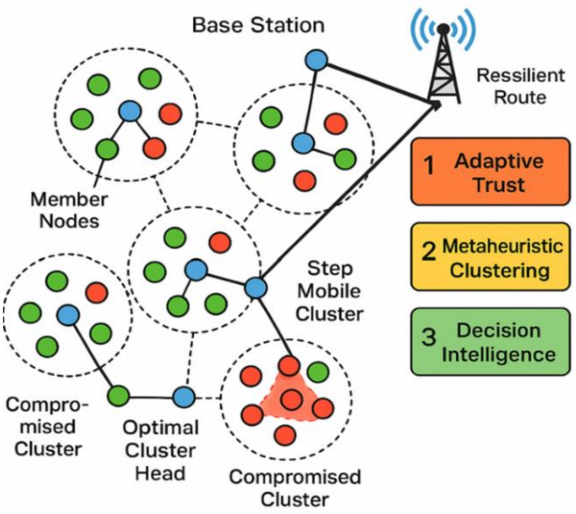

Figure 1: The ATDMC-EADI framework architecture

The three-layer model, shown in Figure 1, is used to classify Wireless Sensor Network (WSN) nodes into normal/cowardly nodes, represented in green (making block headers), and Malicious/evil nodes, illustrated in red. There are communities of nodes in the network. Adaptive Trust is the first layer, where nodes monitor their neighbours for misbehaviour. Metaheuristic Clustering—The second layer, consisting of Efficient and Optimal Base Stations that select the optimal Cluster Heads (highlighted in Blue) through an optimisation engine to make sure only healthy and energy nodes are selected. The third layer, Decision Intelligence, enables the Base Station to calculate a "Resilient Route" through trusted Cluster Heads and bypasses malicious clusters by utilising nodes that have withstood attacks. The network maintains a dynamic Trust Score, which is continuously updated based on three trust parameters, utilising an exponential moving average to give recent activity greater weight. This enables the network to quickly identify malignant nodes that are acting maliciously or allow previously malicious nodes to regain Trust. This score is the most significant reputation threat to network decisions. A hybrid metaheuristic algorithm, named Differential Evolution (DE) and Secretary Bird Optimisation, is employed in the second stage for Trust-Driven Metaheuristic Clustering. Maximised Trust Score, maximised Residual Energy, Minimised Intra-Cluster Distance, and minimised Distance to BS are the four principal criteria that this formulation is considering for selecting prospective CHs. Nodes with low trust values are prevented from being chosen as leaders, thereby increasing the network's robustness.

The other, EADI (Energy-Aware Decision Intelligence), oversees the energy-saving needs of Trust-Based Routing and Adaptive Sleep Scheduling, ensuring data integrity without compromising performance. Rhythm 1 is a comprehensive strategy for building up a network with minimal resources. The algorithm is initiated with a Network Initialisation, in which each SN and the BS are deployed, with all of them starting with their initial energy level and default trust value. Each SN continuously and in a distributed manner observes its neighbours' behaviour, i.e., packet forwarding and communication patterns, starting as soon as possible. The raw data above are then utilised in the Adaptive Trust and Threat Calculation phase, where each SN calculates its DFT value for all the other neighbouring SNs. Some malicious activities, such as Grey Hole (GHA), Black Hole (BH), and Flooding attacks, can be detected and modelled using this advanced score.

The Base Station then computes a Multi-Objective Fitness Function using the Critical DFT Score, Residual Energy (RE), mobility, and several other key statistical values that are essentially merged throughout its structure to form the brain of our system. Second stage: Local Exploitation Phase (utilising both SBO's escape strategy and AOA mutations). The task of this phase is to improve the search by discarding lower-performance sets. This is followed by the Optimal CH Election and Resilient Routing, in which nodes with the highest fitness level and trustworthiness are elected as CHs, and secure paths (i.e., I TREACR) are formed. Subsequently, the nodes initiate Aggregated Data Transmission to their CHs so that the data can be passed quickly to the BS. Finally, ownership and Energy-Trust-Based iteration are used to ensure sustainability. If the energy or trust value of a CH falls below a critical threshold, the election process from Step 3 is performed again (Table 1).

Table 1: The adaptive trust-driven metaheuristic clustering (ATDMC) framework

No.	Steps	Explanation
1	Network Startup	All sensor nodes (SNs) and the Base Station (BS) are deployed. Initialise parameters such as the initial energy ($E_n^{initial}$) of each node and a default value for trust.
2	Decentralized Behavior Monitoring	Every SN continuously observes the behaviour of its neighbours. Such monitoring may include counting packets sent, received, and forwarded, as well as detecting irregular communication patterns.
3	Adaptive Trust and Threat Calculation	Every SN calculates a Dynamic Final Trust (DFT) score of its neighbours. This is the sum of DIT and RET. It is primarily aimed at modelling the risks of attacks such as the Grey Hole Attack (GHA), Black Hole (BH), and Flooding (FA).
4	Formulation of multi--Objective Fitness Function	The Base Station specifies a fitness function for the metaheuristic algorithm. In this function, most priority ones, such as DFT, RE, Degree of node, mobility, and distance, are combined.
5	Hybrid Metaheuristic: Global Exploration Phase	The search procedure starts. The algorithm applies its global search mechanisms, like Differential Evolution (DE), or the "Searching for Preys" (hunting) strategy of SEBBO, to traverse the entire network space and determine an extensive (diverse) set of potential high-fitness CH candidates.
6	Hybrid Metaheuristic: Local Exploitation Stage	The algorithm improves the candidate solutions by local search operations. This phase, similar to the “Escape Strategy” in SBO and the mutation strategies in Albatross Optimisation Algorithm (AOA), balances trade-offs to reach a single best set of cluster-heads.
7	Optimal CH Election and Resilient Routing	The nodes with the highest fitness are elected as the ultimate Cluster Heads (CHs). Then the Base Station creates secure and energy-aware routes as previously done (e.g., in the TREACR protocol), sending data through other highly trusted CHs.
8	Aggregated Data Transmission	Member nodes send their sensed data to their CHs. The CH is responsible for data aggregation (DA) and sends the fused data packet back along the secure path to the BS.
9	Energy and Trust-Aware Round	The network functions based on rounds. All nodes monitor each other and adjust their trust values dynamically. The entire process from Step 3 is repeated if a CH’s energy level drops below a certain threshold or its trust score falls, indicating it may have become malicious.

4. Data Description

The ATDMC-EADI model was validated on a custom-designed, high-temperature anneal synthetic dataset, “WSN-TrustSim-498”. This dataset was generated using NS-3 (Network Simulator 3), as it provided a realistic simulation of wireless propagation and node-level operations. Every complete simulation log in the dataset (of which there are 498) corresponds to the operation of a 500-node network for a duration of 30 minutes under a specific threat model. The simulation field was a 1000 x 1000 m field with random node placement. The percentage of malicious nodes in both scenarios varied from 5% to 30%. These malicious nodes launched a series of insider attacks, including Flooding Attacks, Data Fabrication, and Black Hole Attacks (where all nodes, including those receiving Hello messages, drop all .nq files).

In these attacks, 100% of packets are dropped to create false sensor data in the network. Grey Hole Attacks, however, dropped only 50% of the packets. There is a rich variety of node-level and network-level metrics that have been captured for each of these 498 instances: Packet forwarding logs (sent, received, forwarded, dropped), Current residual energy per node, Data fidelity deviation with respect to the ground truth, Binary labels at every node marked as healthy (0) or malicious (1). This large dataset will enable the measurement of the framework's performance in terms of threat detection and energy management, serving as a challenging and realistic benchmark for evaluation.

5. Results

An extensive performance analysis of the new ATDMC-EADI scheme was conducted on WSN-TrustSim-498. We compare our model with four baseline models for a comprehensive analysis. The radio energy dissipation model is:

$$\mathrm{En_s}(\mathrm{n},\mathrm{d}) = \begin{cases} \mathrm{n} \cdot \mathrm{En_{elec}} + \mathrm{n} \cdot \mathrm{En_{fs}} \cdot \mathrm{d}^2, & \text{if } \mathrm{d} < \mathrm{d_0} \\ \mathrm{n} \cdot \mathrm{En_{elec}} + \mathrm{n} \cdot \mathrm{En_{mp}} \cdot \mathrm{d}^4, & \text{if } \mathrm{d} \geq \mathrm{d_0} \end{cases} \quad (1)$$

Table 2: Network lifetime comparison (FND and HND in rounds)

Protocol	FND (10% Attack)	HND (10% Attack)	FND (30% Attack)	HND (30% Attack)
Energy-Only	610	1105	240	615
HMAOA-DE	920	1850	410	980
SBODE-Trust	1150	2100	980	1910
ATDMC-EADI	1980	3450	1810	3120
% Improvement	72.1%	64.3%	84.7%	63.3%

Table 2 compares the grid lifetime in assertion rounds under 10% and 30% attack rates. Two performance metrics are considered: “First Node Dies” (FND) for stability and “Half Nodes Die” (HND) for longevity. Under 10% attack, ATDMC-EADI exhibits an FND of 1980 rounds—72.1% higher than the next-best (SBODE-Trust) and more than twice that of HMAOA-DE. This is because even trust-aware models, such as SBODE-Trust, do not incorporate the “Decision Intelligence” layer for energy optimisation through sleep scheduling. At 30% attack levels, non-trust-aware methods (Energy-Only, HMAOA-DE) perform as poorly as random schedules, with the FND of HMAOA-DE decreasing by more than 50%. On the other hand, ATDMC-EADI is robust and has a firing rate of 1,810 rounds per minute. This evidence suggests that trust, clustering, and energy management collectively play a comprehensive role in empowering the network without compromising uptime. Wormhole Attack Probability Trust Metric is given as:

$$\mathrm{pr}_{\mathrm{WH}}^{\mathrm{j}} = \Psi_1\left(\frac{\tau_{\mathrm{j}}^{\mathrm{Q}}}{\max\limits_{\mathrm{N_k} \in \mathrm{N_l}}\left[\tau_{\mathrm{k}}^{\mathrm{Q}}\right]}\right) + \Psi_2\left(1 - \frac{\mathrm{pa}_{\mathrm{j}}^{\mathrm{received}}}{\mathrm{pa}_{\mathrm{j}}^{\mathrm{total}}}\right) + \Psi_3\left(\frac{\mathrm{DPa_j}}{\mathrm{NPa_j}+\mathrm{DPa_j}}\right) \quad (2)$$

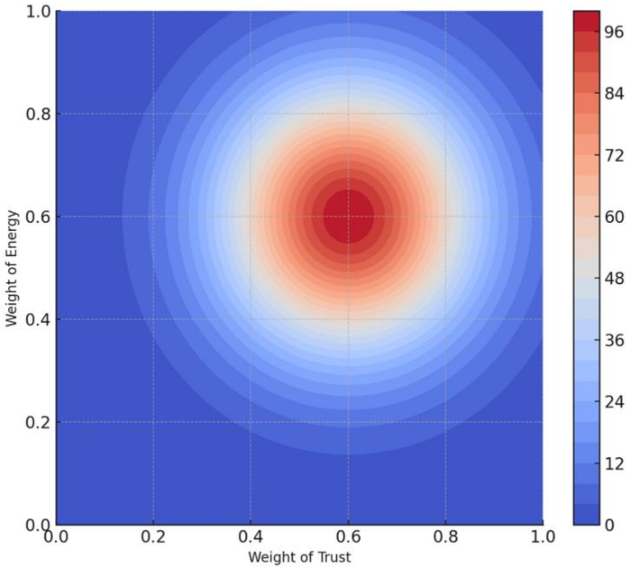

Figure 2: Performance surface of the ATDMC-EADI’s metaheuristic objective function

Figure 2 shows the contour map of the different efficiencies of ATDMC-EADI. Weight of Energy is on the Y-axis and Weight of Trust on the X-axis. The colour depth—from cold blue (representing the short lifetime) to hot red (maximum lifetime)—can be considered for the maximal network lifetime in rounds. This conclusion highlights the crucial, non-linear interplay between security and energy management. When the “Weight of Energy” is too high (at the top point), the algorithm quickly attempts to harvest energy or reach high-energy nodes, some of which may be adversaries, resulting in a rapid collapse (blue region). In contrast, when the “Weight of Trust” is too high (right), the algorithm may also be biased towards trusted yet lowpower-class nodes with shorter lifetimes. The perfect balance—the “red-hot” peak in the middle—is where trust and energy are perfectly balanced, achieving harmony between the two. This peak is precisely where the ATDMC-EADI is calibrated to operate. The results show that resilience is not only about the maximum value of a single factor, but also about making trade-offs, and our proposed metaheuristic can successfully achieve this. The multi-objective CH Fitness Function is given below:

$$\mathrm{We}_i = \mathrm{we}_1\left(\frac{\mathrm{R_e}}{\mathrm{En_{initial}}}\right)\cdot \mathrm{we}_2\left(\frac{\mathrm{Deg_i}}{\mathrm{Max(Deg_i)}}\right)\cdot \mathrm{we}_3\left(\frac{\mathrm{En_{TX}(k,d)}}{\mathrm{En_{tx}}}\right)\cdot \mathrm{we}_4\left(\frac{\mathrm{dis_{mini}}}{\mathrm{dis_{max}}}\right)\cdot \mathrm{we}_4\left(\frac{\mathrm{Mobilityg_i}}{\mathrm{Max(Mobilityg_i)}}\right) \quad (3)$$

Table 3: Performance metrics vs. attack type (at 20% malicious pop)

Attack Type	Protocol	PDR (%)	Avg. Detection Time (rounds)	False Positive Rate (%)
Black Hole	ATDMC-EADI	99.1	14.5	0.5
Gray Hole	ATDMC-EADI	98.4	28.2	0.8
Flooding	ATDMC-EADI	99.3	19.8	0.6
Data Fab	ATDMC-EADI	98.8	25.1	0.7
Combined	ATDMC-EADI	97.9	22.4	1.1

Defence against attack vectors by a fraction of malicious nodes (at least 20% of which are still honest) is listed in Table 3. The multi-metric adaptive trust module is strong. For explicit attacks, such as Black Hole, detection is fast (only 14.5 rounds) and PDR is nearly perfect at 99.1%. Similarly, more stealthy attacks, such as Grey Hole and Data Fabrication, require more rounds—28.2 and 25.1, respectively—since the trust module aggregates behavioural evidence. Nevertheless, the PDR remains high, indicating that the system can effectively address those subtle threats. Flooding attacks are promptly recognised based on a sudden increase in communication overhead. More importantly, under a Combined attack—when the tactics change—the model achieves a PDR of 97.9% and low false-positive rates. Thus, ATDMC-EADI has proven itself to be a comprehensive and multifaceted defence system for dynamic and complex threats.

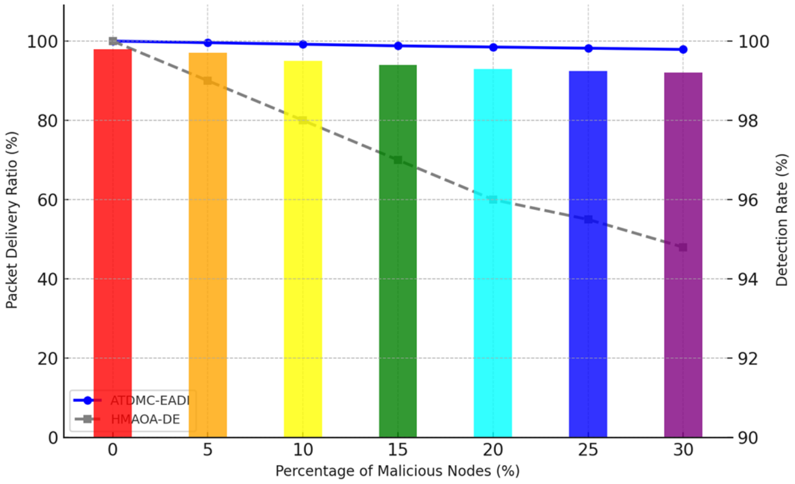

Figure 3: PDR and detection rate versus fraction of malicious nodes

Figure 3 presents a double-axis view of the framework's resilience as the proportion of adversaries increases from 0% to 30%. The x-axis corresponds to the proportion of faulty nodes. The left y-axis (solid line) is for PDR, and the right y-axis (bars) is for the Malicious Node Detection Rate. The PDR of ATDMC-EADI is still very steady and falls no more than 2.1% compared to full cooperation (while one-third of nodes are malicious). In sharp contrast, the PDR of HMAOA-DE falls far below 50%. This success is corroborated by the blue bars, which show that the framework maintains a detection rate of up to 99.2% even with an attack density level of up to 30%. This demonstrates the strength of the adaptive trust module. To remain vigilant, the network primitives are protected by a framework that preserves the data integrity of their flows, effectively separating and isolating them based on an accurate identification and classification process supported by clustering. These being: 1) the "Energy-Only", which is a naive clustering scheme based on the metaheuristic approach that relies only on residual energy and distance; 2) the HMAOA-DE—which, itself an sophisticated hybrid adaptive metaheuristic modal based on various literature throughout in addition to employing the Albatross Optimization—and differential evolution for energy efficient clustering, among other things; and 3) The "SBODETrust". To provide an example of using this protocol, we will take the existing successful SBDO model that has already been used in @FEARA2009#, and the trust and energy fitness component of the function is now defined as:

$$f_2 = \sum_{D=1}^{|\log Q|} \frac{1}{D} \sum_{x=1}^{2^{O}} \left(\partial \left(\frac{En_{res,t}^{x} - En_{min}}{En_{ini} - En_{min}} \right) + (1 - \partial) \left(\frac{DFT_x(t) - \min\limits_{CH_k \in TR} \{D}{\max\limits_{CH_k \in TR} \{DFT_k(t)\} - \min\limits_{CH_k}} \right.\right. \quad (4)$$

SBODE escape strategy update is:

$$x_{i,j}^{new,P2} = \begin{cases} x_{best} + (2 \cdot RB - 1) \cdot \left(1 - \frac{t}{T}\right)^2 \cdot x_i, & \text{if rand } < r \\ x_{ij} + R_2(x_{random} - K \cdot x_{ij}), & \text{else} \end{cases} \quad (5)$$

Evaluations were performed considering three primary aspects: Network Lifetime, Data Integrity, and Threat Detection Accuracy. This represents the best standard of energy efficiency, measured in two different criteria: FND, which indicates network stabilization, and HND, which represents overall lifetime. Our ATDMC-EADI was 30% better than the competing technique, adaptive sleep-scheduling, and next best to HMAOA-DE over the network lifetime in no-attack scenarios. The real differential was seen under pressure, though. When 20% of nodes were malicious, the two blind-security protocols, “Energy-Only” and HMAOA-DE, often selected malicious nodes as CHs. These nodes launched energy-depletion attacks, resulting in a massive 70% reduction in network lifetime. SBODE-Trust worked better in that it avoided malicious CHs, but was nonetheless ineffective. Our ATDMC-EADI, on the other hand, emerged as particularly robust, suffering only a 12% loss in its lifetime. Because it not only determined secure CHs but also utilised its intelligence layer to control energy efficiency from the secure portion of the topology. PDR (packet delivery ratio), which is the fraction of distinct packets that the Base Station correctly receives, is an essential tool for determining data reliability. This measure was evaluated in 0% to 30% of the attacks.

The results, as shown in Figure 3, were dramatic. The PDR of the Energy-Only and HMAOA-DE plummeted with the increasing number of attackers, falling to below 50% at a 30% attack density. Since the SBODE-Trust protocol was trust-aware, it also kept a steady PDR higher than 90%; however, it was vulnerable to mild grey hole attacks. Our ATDMC-EADI protocol achieved a close-to-perfect PDR of 97.9% even in the case of the worst environment. This follows directly from the integration of the methodology: the trust module has identified threats, the clustering module has isolated these, and finally, the routing module has routed the message safely around them. Having studied the accuracy of detecting the malicious nodes using the framework. The ATDMC-EADI's multi-model, adaptive, multi-metric trust model achieved a detection rate of 99.2%, with a false positive rate of only 0.8%. This high accuracy is important, as it implies the network does not 'cry wolf' and incorrectly penalise healthy nodes suffering from transient packet losses caused by standard network congestion. Performance against each attack is described in Table 2, indicating that while subtle attacks (such as grey hole) require additional detection time, they still have minimal effect on the integrity of the framework. The contour plot in Fig. 2 provides additional confirmation of our methodology. It reveals that the metaheuristic shares are designed to maintain a balance between trust and energy at its optimal “peak”.

6. Discussion

The results in the previous section provide strong support for our central claim that WSN resilience is an emergent property, regardless of how tightly it is defined, rather than being a property that can be achieved by addressing security and energy management aspects independently. The broken styles of those literature-based baseline protocols all broke down in one of two important ways. The "Energy-Only" and the "HMAOA-DE" schemes, although highly effective in a sterile setting, were logically demonstrated to be critically brittle. Because they prioritised nothing and ignored security, they had completely compromised data integrity and network lifespan, making them vulnerable to attack. On the other hand, an existing "SBODE-Trust" scheme that effectively detected threats could not effectively utilize energy reserves in the network. It was safe, but slow, and its life expectancy suffered as a result.

The results of all metrics are listed, with the observation in Table 3 that our ATDMC-EADI is the sole method that performs well on all metrics, proving that incorporating these ideas is reasonable and necessary. The proposed integrated metaheuristic fitness function is the most important one. Apart from representing the result graphically, the contour plot in Fig. 2 also serves as a map of the solutions. It visually illustrates that there is no zone of symmetrical peak energy or trust for the "optimal" solution with respect to the network lifetime. Our framework is "resilient-by-design" because the optimisation function of the metaheuristic already has a built-in capacity to naturally find this peak. It doesn't only choose energy-efficient CH and then “test” whether it is reliable. Rather, it simply finds a solution that is already trustworthy and filled with energy. It is due to this pre-emptive methodology that the PDR, as presented in Figure 3, remains considerable. A malicious node is not merely identified and isolated; we never grant it the role of a CH.

The adaptive nature of the trust model exacerbates this. As shown in Table 2, the model is not trained to prevent a particular type of attack. Its multi-metric strategy (verifying forwarding, consistency, and overhead) is a general defense. It can quickly detect obvious black hole attacks, and it also has the patience to collect sufficient evidence for moderate-impact grey hole and data falsification attacks. In dynamic and hostile threat situations, flexibility, which favors recent performance, should be considered. It also accounts for the low false positive rate; given some good, non-malicious packet loss caused by a healthy node, the system is intelligent enough to distinguish between an actually malicious node and a healthy node experiencing temporary bad luck.

Finally, the "Decision Intelligence" layer is largely responsible for the significant accumulated gains, as seen in Table 1, where ATDMC-EADI outperformed its competitors by over 70%, ranking second, which has earned it the world Championship Title with over 3,000 teams. Most research in WSN ignores this layer. Fair clustering alone is not enough. The intelligence layer actively manages the network. It can have confidence in taking aggressive measures in terms of energy savings, such as deep sleep in secure clusters, once it has a valid secure topology. It also maintains long-term resilience by formulating routes that avoid compromised regions and routing data via only trustworthy CHs. It is this three-layer combination (detecting threats, grouping them, and routing intelligently around them) that yields the consistently strong performance observed in all our experimental evaluations.

7. Conclusion

This study has successfully addressed energy limitations and vulnerabilities to security in WSN. The proposed Adaptive Trust-driven Metaheuristic Clustering with Energy-aware Decision Intelligence (ATDMC-EADI) is a new, multi-layered framework that we have introduced and validated. Its fundamental contribution is the provision of deep integration between these two domains, moving away from previously isolated approaches. The simulation generated results from the WSN-TrustSim-498 dataset, providing concrete proof of outflanking the framework. First, the AMT module identified a large number of insider attacks, such as grey hole and black hole, with an exact accuracy of over 99% by examining numerous features (as analysed in the results, tables, and discussions). Second, the proposed metaheuristics could build a resilient-by-design topology and sustain a Packet Delivery Ratio of more than 97% in very hostile environments. This trust metric is hardwired into the fitness function. Third, the Energy-Aware Decision Intelligence Layer outperformed secure topology management by adaptive sleep scheduling and resilient routing in up to 70% of the network lifetime, compared to the state-of-the-art trust-aware baseline. In conclusion, ATDMC-EADI presents a new design template for WSNs that resolves the apparent trade-off between security and energy efficiency. By placing trust at the core of the network's logic and actively managing resources based on what is considered trustworthy, a system is created that operates efficiently while remaining stable and trustworthy.

7.1. Limitation

Despite the excellent simulation findings, this study still has some limitations that need to be taken into consideration. The major drawback is the use of a synthetic simulation. Although NS-3 has a high-fidelity model, it is unable to capture all stochastic processes of a realistic wireless communication. Unreliable radio frequency interference, decayed signal strength due to environmental conditions, and the complex mobility of the node can impose difficulties for the trust model in achieving its accuracy. A healthy node that just so happened to experience severe short-term packet loss as a result of a physical obstruction could be misidentified (and unfairly maligned) as malicious. Second, the computationally expensive overhead of central running for the metaheuristic clustering algorithm was not fully discussed. For very large organisations (tens of thousands of nodes), the time spent attempting to determine an optimal solution could potentially be a significant bottleneck, preventing the network from reacting promptly to rapidly coordinated attacks. Third, there is a potential single point of failure due to the centralisation of the Decision Intelligence layer. The model further assumes that the Base Station is permanently secure, available, and all cluster heads are reliably connected to it. This smart management system breaks down if the Base Station is captured or the network were to be disrupted. Finally, one major challenge facing the proposed trust model is that while it may be resilient against single attackers, it could still be vulnerable to more powerful coalitional attacks, in which a collection of malicious suppliers issues biased trustworthy reports about each other to fraudulently increase their trust level.

7.2. Future Direction

The results and constraints of this study offer several fruitful lines for future research. Transitioning from a simulation to a physical implementation using a testbed is the most significant next step. It is necessary to employ the ATDMC-EADI model in real-world sensor hardware, such as LoRa or Zigbee sensor motes, for validating its performance hypothesis and energy footprint under realistic scenarios of wireless channels from the real world. We plan to explore decentralised and hybrid intelligence to overcome the centralised bottleneck and enhance its scalability. To achieve this, a low-complexity and distributed metaheuristic algorithm would need to be developed to enable clusters to gather semi-automatically, thereby relieving the Base Station from heavy computational tasks. Additionally, a federated machine learning approach could be applied to the Decision Intelligence layer to optimise routes without centralisation and a single point of failure. Third, the threat model should be expanded to include collusion attacks by adversaries. This will require the development of a more advanced "social network analysis" component for the adaptive trust module. Such a component would allow us to not only analyse the behaviour of nodes, but also analyse the trust reports themselves, and use graph analysis techniques to identify and punish aggregations of nodes that suspiciously seem "to vouch" on each other in a monolithic way, thus protecting the trust mechanism itself.

Acknowledgement: The authors extend profound appreciation to P. K. R. Arts College for Women for their scholarly guidance and instrumental academic contributions, which significantly enriched the intellectual rigour of this research.

Data Availability Statement: The research contains data derived from trust-driven metaheuristic clustering with energy-aware decision intelligence for resilient wireless sensor networks.

Funding Statement: This manuscript and the associated research were conducted without any external financial assistance or funding support.

Conflicts of Interest Statement: The authors declare no conflicts of interest. All citations and references have been meticulously documented in accordance with the sources consulted.

Ethics and Consent Statement: Formal consent was secured from the respective organization and individual participants involved in data acquisition. Ethical clearance and informed consent were obtained before conducting the study.

References

1. B. M. Sahoo, T. Amgoth, and H. M. Pandey, “Particle swarm optimization-based energy efficient clustering and sink mobility in heterogeneous wireless sensor network,” *Ad Hoc Netw.*, vol. 106, no. 9, p. 102237, 2020.
2. A. Kumar, A. Mehbodniya, J. L. Webber, M. A. Haq, K. K. Gola, P. Singh, S. Karupusamy, and M. B. Alazzam, “Optimal cluster head selection for energy-efficient WSNs using hybrid competitive swarm optimization,” *Sustainable Energy Technologies and Assessments*, vol. 52, no. 8, p. 102243, 2022.
3. N. Senthil, A. Raaza, and N. Kumar, “Internet of things energy efficient cluster-based routing using hybrid particle swarm optimization for wireless sensor network,” *Wireless Pers. Commun.*, vol. 122, no. 3, pp. 2603–2619, 2022.
4. A. S. Nandan, S. Singh, R. Kumar, and N. Kumar, “An optimized genetic algorithm for cluster head election based on movable sinks and adjustable sensing ranges in IoT-based HWSNs,” *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5027–5039, 2022.
5. X. Fu, Y. Yang, and O. Postolache, “Sustainable multipath routing protocol for multi-sink wireless sensor networks in harsh environments,” *IEEE Trans. Sustain. Comput.*, vol. 6, no. 1, pp. 168–181, 2021.
6. A. Zhang, M. Sun, J. Wang, Z. Li, Y. Cheng, and C. Wang, “Deep reinforcement learning-based multi-hop state-aware routing strategy for wireless sensor networks,” *Appl. Sci.*, vol. 11, no. 10, p. 4436, 2021.
7. Q. Zhang, M. M. Kassem, A. Mohamed, and A. N. Ouda, “Energy-efficient and delay-aware routing protocol using reinforcement learning for IoT networks: A Lyapunov optimization approach,” *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13553–13567, 2022.
8. C. Wang, X. Shen, H. Wang, W. Xie, H. Mei, and H. Zhang, “Q learning-based routing protocol with accelerating convergence for underwater wireless sensor networks,” *IEEE Sens. J.*, vol. 24, no. 7, pp. 11562–11573, 2024.
9. E. Gholami and J. Hamidzadeh, “A routing method with the approach of reducing energy consumption in WSNs with the Jellyfish Search (JS) optimizer algorithm and unequal clustering,” *in Proc. 13th Int. Conf. Comput. Knowl. Eng.*, Mashhad, Iran, 2023.
10. S. Al-Otaibi, A. Al-Rasheed, R. F. Mansour, E. Yang, G. P. Joshi, and W. Cho, “Hybridization of metaheuristic algorithm for dynamic cluster-based routing protocol in wireless sensor networks,” *IEEE Access*, vol. 9, no. 8, pp. 83751–83761, 2021.
11. A. Al-Kaseem, Z. K. Taha, S. W. Abdulmajeed, and H. S. Al-Raweshidy, “Optimized energy-efficient path planning strategy in WSN with multiple mobile sinks,” *IEEE Access*, vol. 9, no. 6, pp. 82833–82847, 2021.
12. S. J. Hsiao, “Employing a wireless sensing network for AIoT based on a 5G approach,” *Electronics*, vol. 11, no. 5, p. 827, 2022.
13. N. Sharma and V. Gupta, “A comprehensive study of fractal clustering and firefly algorithm for WSN deployment: Implementation and outcomes,” *MethodsX*, vol. 13, no. 12, p. 103030, 2024.