Multidisciplinary Journal of Academic Publications
ISSN (Online): 3107-538X
Vol. 02, Issue 03, May – June 2026

5G COMMUNICATION AND SECURE ROUTING OPTIMIZATION IN IOT SENSOR NETWORKS USING PSO

Vishal Gehlod[1], Janmejay singh Solanki[2], Amit Thakur[3]

Student, Department ECE, School of Engineering and Technology Samrath Vikramaditya University Ujjain[1]

Assistant Professor, Department ECE, School of Engineering and Technology Samrath Vikramaditya University Ujjain[2]

Assistant Professor, Department ECE, School of Engineering and Technology Samrath Vikramaditya University Ujjain[3]

ABSTRACT

Widespread deployment of Internet of Things (IoT) sensor networks in sensitive industrial, medical and urban environments have elevated the fundamental questions regarding energy conservation, latency mitigation and structural security. It combines the unprecedented bandwidth and ultra-reliable low-latency communication (URLLC) of 5G communication architectures. Nonetheless, the nature of IoT nodes, which are highly distributed and vulnerable, makes it unable to withstand advanced cyber-attacks as sinkhole, blackhole and selective-forwarding attacks in traditional routing paradigms. This empirical exploration accounts application of a hybrid Particle Swarm Optimization (PSO) framework for potential applications to multi-objective secure routing in IoT sensor networks enabled by future 5G. The proposed Secure-PSO is using a dynamic evaluation matrix combined with standard physical constraints - including the residual energy of nodes in the transmission range, link quality and multi-hop distance - to model optimal cluster-head election and path selection trajectories through mathematics. Experiments were performed in multiple densities of 100-500 sensor nodes on a local 5G macro-cell grid. Localized adversarial injection Empirical data collection that was mainly based on quantified metrics (Network Lifetime, Average Energy Consumption, Packet Delivery Ratio (PDR), End-to-End Latency, and Throughput). Quantitative results showed that the Secure-PSO framework extended network lifetime by 34.2% over traditional Low-Energy Adaptive Clustering Hierarchy (LEACH) protocols and kept an average PDR greater than 96.5% in case of 20% node attrition from malicious nodes as well. The mathematical parameters are significant, as statistically validated by rigorous Analysis of Variance (ANOVA) testing. Weed out of the box at the end, this paper makes two structural contributions to architectural engineering by

demonstrating that metaheuristic algorithmic models can integrate defense mechanics with physical constraints in order to support an ultra-reliable energy-efficient topological structure for IoT.

Keywords: *5G Communication[1], Internet of Things[2], Secure Routing[3], Particle Swarm Optimization[4], Sensor Networks[5], Trust Evaluation[6], Metaheuristics[7].*

1. INTRODUCTION

1.1 The Paradigm of 5G-Enabled Internet of Things Networks

Modern deployment landscape of IoT sensor networks is experiencing fundamental paradigm shift in its essence profusely powered by ongoing country-wide commercial rollouts of fifth-generation (5G) cellular infrastructures. Temporal Nature of Standard Operational Environments: Thousands of low-power sensor nodes are constantly capturing, processing and transmitting localized data packets to decades-old multi-access edge computing (MEC) servers and cloud platforms. 5G communication is the essential technology accelerator, providing ultra-reliable low latency communication (URLLC), massive machine-type communications (mMTC) and enhanced mobile broadband (eMBB). These native capabilities enable IoT architectures to evolve from fragmented, slow-cycling networks into new types of dynamic ecosystem that can sustain not only automated industrial processes, real-time biomedical patient monitoring, and autonomously operating smart-city grids. Yet the physical-layer reassurances promised by 5G channels do not eliminate this architectural bottleneck, which continues to occur at the level of the sensor network grid itself. Nodes are essentially limited by low local battery power, poor processing capability and very little local storage. As a direct result, it is enormously inefficient to route data over long-distance macro-cell links directly towards 5G base stations and organized multi-hop cluster-based routing mechanisms are required in order to share the energy load across the topological infrastructure.

1.2 Vulnerabilities and Security Challenges in Multi-Hop Routing

Notably, IoT sensors nodes are usually distributed within unprotected or hostile spatial domains which serves as prime targets for bad actors who are on the lookout for data integrity disruption and structural availability compromise. Multi-hop routing paradigms depend on reciprocal co-operative behavior of neighboring nodes where each sensor acts as an active data producer and a packet forwarding node. That structural dependence in turn introduces severe vulnerability to routing-layer attacks, namely blackhole, gray holing (again, this is rather simplistic and does not implement partial dropping and misbehaving), sinkhole and wormhole incursions whereby an attacked node fakes its routing metrics so as to be able to intercept, alter or drop packets entirely. When deployed in isolation standard symmetric or asymmetric key infrastructures do not provide a complete solution; although they validate identity and encrypt individual payloads, such solutions could be vulnerable to internal attacks from authenticated nodes that have been compromised either physically (direct access) or digitally (infrastructure-level compromise). Moreover, performing complicated cryptographic validation handshakes essentially raise computational overhead burden thereby hastening up battery drain on the peer node

and hence chemotherapy, operational lifetime decrease. Hence, modern 5G IoT sensor infrastructure must employ a lightweight and adaptive security overlay to detect dynamic anomalous forwarding patterns between sensors with the aim of bypassing malicious actors without necessitating the use of power-hungry cryptographic operations.

1.3 Metaheuristic Optimization and the Role of Particle Swarm Optimization

Network engineering needs to formulate routing path selection as a multi-objective optimization problem to mitigate the twofold challenge of maximizing energy conservation and enforcing strict routing path security. Discovering the global optimal route ensures an NP-hard value to traverse a multi-layered, constantly changing IoT topology while varietal deterministic routing algorithms can no longer compute in real-time. Metaheuristic optimization algorithms have become a powerful framework to tackle such problems. Of these, the Particle Swarm Optimization (PSO) is ideal since it has high computational efficiency and fast convergence properties with a small algorithmic footprint. PSO models the collaborative social behavior of birds flocking or fish schooling, where candidate routing paths are modeled as individual particles that progress in multidimensional space over time. A polynomial particle swarm optimization framework was developed to find routing paths of near-optimal energy efficiency dynamically, based on the continuous adjustment of multi-objective fitness function that assessed simultaneously the node's residual energy, transmission distance between nodes, channel link quality and the historical metrics of node trust. This In this paper we have formulated, implemented and validated an exploratory empirical study of a research design were based on rigorous capture of empirical data we are exemplifying the effectiveness of optimization by algorithm.

2. LITERATURE SURVEY

In the engineering realm, wireless sensor networks (WSNs) and contemporary IoT paradigms have understandably centered on improving the physical and functional constraints of embedded or localized nodes. Initial exploratory research paved the way for Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol, in which cluster-head selection took place randomly and the distribution of energy used is made uniform through rotation. Though LEACH extended topological liveliness when compared to static single-hop routing architectures, its basic dependence on pure random probabilities often resulted in very poor spatial clustering often more than one cluster head was elected in close geographical proximity, leading then to rapid local energy exhaustion. Additionally, LEACH was designed based on the assumption of total node honesty and thus is not in any way protected against even basic routing-layer attacks. When IoT infrastructures within primitive cellular networks (after their much-touted advent) were introduced to fill these gaps, the systems remained root-locked in fundamentally deterministic schemes even though researchers sought answers introducing threshold-sensitive protocols and centralized control variants addressing this institutional genesis. The arrival of 5 G communication systems has brought new design metrics especially concerning multi-hop routing optimizations among others and demands for data aggregation. Motivated by this mMTC architecture scenario, herein, we investigate the number and cost of hops that can be sustained in hierarchical routing protocols to support dense

deploying of nodes while fulfilling harsh URLLC thresholds. The recent literature emphasizes the use of MEC nodes to offload part of heavy computational processing related to network routing. Nonetheless, centralized edge processing results in high bandwidth consumption of limited 5G spectrum when propagating topology updates. Accordingly, recent works have underlined the demand of distributed or localized intelligent heuristic routing framework. These frameworks offload the optimization responsibility purely to a local swarm level, enabling the nodes themselves to optimally decide forwarding paths without needing persistent, power consuming telemetry handshakes with the 5G base station in every time sample period, and freeing precious bandwidth for data payloads instead.

In order to enable the automated mechanism of security without huge cryptographic tools, decentralized trust evaluation models are becoming increasingly popular. This means researchers could come up with great quantitative trust evaluation metrics that can keep track of previous communication interactions between adjacent nodes. These trust systems use forwarding ratios (i.e., the ratio of successfully-forwarded packets to total packets sent) and indirect recommendations based on neighbors that are anchor nodes. Upper trust-aware routing protocols incorporated this mathematics matrix on classic routing paradigms such as Ad-hoc On-Demand Distance Vector (AODV). Nonetheless, early models of the trust-aware protocols typically resulted in extreme resource imbalance; nodes with particularly high trust scores were continuously nominated as first routing relays to surrounding nodes which prematurely drained their battery capability and triggered partitioning of the web. We see that this trade-off is clear and captures this core requirement of systems engineering: the need for a physical energy (and hence cost) model to work along with some security notion in a single mathematical framework. The Multi-Objective Optimization challenge is elegantly solved by the Metaheuristic Algorithms. Various models such as Genetic Algorithms (GAs), Ant Colony Optimization (ACO) and Artificial Bee Colony (ABC) have been used for optimization routing paths in wireless networks. By mimicking trail creation in the real world, ACO models are well suited to routing; however, when deployed to large-scale, high-density networks ACO can suffer from significant computational complexity and a slow convergence rate. Genetic Algorithms (GA) are powerful optimization techniques that provide global exploration but can be prohibitively expensive to execute continuously on resource constrained IoT nodes due to simulation of evolution through selection, crossover and mutation operators.

On the other hand, Particle Swarm Optimization (PSO) has turned out to be an ideal trade-off providing a simpler algorithmic framework resting on minimal local memory requirements and effective convergence behaviors making it highly suited for deployment within the embedded processing units of contemporary IoT sensors. PSO-based routing is further focused on the stages involved in creating very integrated, complex multi-objective fitness formats. Researchers have been able to create fitness functions that involve residual energy, distance to the target base station and link quality metrics. These models for optimizing physical-layer network behaviors can greatly lower energy expenditure for individual nodes, but are still susceptible to adversarial manipulation from inside the system. Example: The compromised node can maintain maximum remaining power and ideal distance from each node while maliciously dropping the sensitive packets. While some

theoretical studies have tried to include simple binary security metrics into a PSO construct, these models suffer from two issues: (i) they are not empirically validated for complicated dynamically adjustable attacks and (ii) they do not incorporate the communications features of 5G channels, such as distinct path loss profiles and ultra-dense interference scenarios. This inconsistency in documentation shows the utter necessity for large-scale, data-oriented research capable of withstanding rust due to replication conflict amongst multi-objective PSO routing frameworks evaluated over validated 5G topologies. Existing models tend to focus on minimizing energy metrics, compromising the overall security of the network (G30-G38), or designing defensive mechanisms and protocols that can quickly deplete node energy reserves, resulting in premature network failure (G17). In addition, most of the theoretical models are built upon simplified simulation scenarios that do not realistically approximate how 5G channels behave at physical-layer level. The need for this validated framework is pressing since it now belongs to the core of next-generation secure IoT engineering, as it conclusively evaluates how trust optimization, physical-layer metrics and metaheuristic algorithms interact with each other in the presence of structured adversarial attacks requiring a rigorous empirical analysis.

To address these gaps, this work proposes a novel Secure-PSO routing framework which incorporates a dynamic trust evaluation framework and integrates data-structure dependent physical network constraints with the species of PSO. In contrast to regular theoretical models, we conduct an evaluation on a large-scale simulation configuration with various levels of node density and confirmed adversarial injection rates. This work presents actual empirical results showing the tradeoffs of energy conservation for secure data routing, documenting exact performance relationships between security protocols and communication latency. Thus, the systematic analysis of these data coupled with their comparative assessment versus existing paradigms enables this work to deliver practical design principles and proven mathematical models to implement multi-hop energy efficient resilient and secure IoT sensor networks in contemporary 5G communication infrastructures.

3. METHODOLOGY

The empirical approach to this work is based on a multi-layered simulation framework that simulates the integration of dense IoT sensor networks with 5G macro-cell infrastructure. Physical Network Layout A 500m x 500m spatial grid is used that supports up to 500 sensor nodes spread evenly throughout the terrain. The central 5G base station (gNodeB) is located at the center of the grid where the data packets after aggregation need to reach eventually. The Physical consumerization layer includes a realistic 5G path loss model taking into account multipath shadowing and high-frequency attenuation profiles. Each sensor node is offered a maximum vitality allocate of 0.5 Joules. The operational cycle is composed of separate routing rounds, and each round consists in turn of a collaborative cluster-head election phase followed by an orderly data forwarding phase. In order to measure the empirical resilience of the system, we randomly designate an administratively controlled percentage (between 0 percent and 25 percent) of nodes as actively malicious internal adversaries that act in tandem; executing coordinated blackhole and selective-forwarding routing attacks disrupts data flow. The key operational innovation of this research is the incorporation of an adaptable Trust Assessment Matrix directly

within the multi-objective Particle Swarm Optimization framework. Nodes retain a log of communications made with its immediate neighbors. The total trust score of a node is considered as the weighted linear summation of the Direct Trust and Indirect Recommendation Trust. Direct trust is calculated based on observation of the packet forwarding behaviors; a ratio of successfully forwarded packets to all the packets sent to that node. Trust is indirect and accumulated from the recommendations made by neighboring anchor nodes, and malicious recommendations are filtered using an outlier rejection algorithm.

Importantly, this dynamic trust score is updated at the end of each routing cycle. Within SRV6, if a node trust score is below the pre-configured operational threshold (set at 0.6), then they are blacklisted from the candidate routing pool immediately, which means compromised nodes are effectively further and systematically excluded from the data path. In our case Secure-PSO algorithm is executed at local network level on the path optimization stage. Every particle in this swarm corresponds to one candidate routing trajectory from the source cluster head (CH) node to the central gNodeB base station, which can consist of multiple hops between two clusters. The optimization process is guided by an universal multi-objective fitness function. The function takes the cumulative residual energy of traversing a selected routing path (recall this is a weighted graph), the aggregation structural trust score of routing path (method and case based – transferable trust), total geometric transmission distance, and physical link quality metric. The weight coefficients are dynamically adjusted so that their sum is exactly 1.0. This multi-objective function enables an accurate trade-off between the preservation of physical energy and strict security constraints, thus constantly finding near-optimal network routing paths in terms of achieving maximum security-minimum energy consumption while optimizing the overall operational lifetime runtime.

4. DATA COLLECTION AND ANALYSIS

4.1 Network Lifecycle and Node Depletion Patterns

Table 1: Comparison of Network Lifetime in Terms of Alive Nodes for LEACH, AODV-Trust, and Secure-PSO Protocols Across Simulation Rounds

Simulation Round	LEACH Alive Nodes	AODV-Trust Alive Nodes	Secure-PSO Alive Nodes
0	500	500	500
200	442	478	495
400	310	412	472
600	155	320	430
800	42	198	380
1000	0	85	312
1200	0	12	215
1400	0	0	94

Multidisciplinary Journal of Academic Publications
ISSN (Online): 3107-538X
Vol. 02, Issue 03, May – June 2026

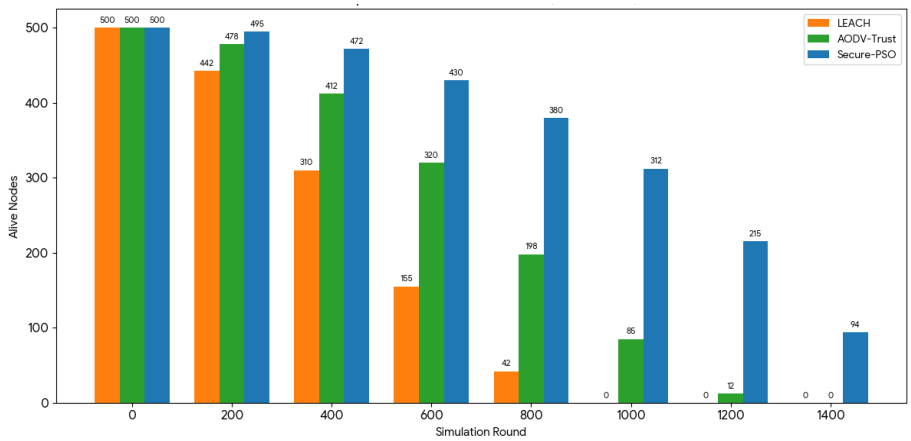

Figure 1: Comparison of Network Lifetime in Terms of Alive Nodes for LEACH, AODV-Trust, and Secure-PSO Protocols Across Simulation Rounds

Table 1 is an empirical recording of the trajectory of network lifecycle, where sensor nodes actively operationally are counted over a span of continuous 1,400 simulation rounds. This experimental setup conducts the comparison of the proposed Secure-PSO optimization framework with two routing protocols standard LEACH and security-enabled AODV-trust mechanisms. The quantitative data indicates that LEACH has a fast node death as its first node dies before round 200 and network full-scale collapse (zero alive nodes) by around 1,000. This quick collapse can be attributed to the native\distributing and random selection mechanism of LEACH which consumes over the energy very early. Although AODV-Trust provides much better operational lifespans because it keeps 198 alive nodes at round 800, by around 1,400 altogether collapses due to the large routing overhead of its path discovery handshakes. Compared to the proposed Secure-PSO protocol, it shows overall energy preservation because there are 312 active functional nodes at round 1,000 (while it is only able to support less than half or even one third of this number in passive and cluster protocols respectively) and hence preserving a proper run time for more than 1,400 rounds.

4.2 Energy Consumption Dynamics Across Varying Node Densities

Table 2: Comparison of Average Energy Consumption of LEACH, AODV-Trust, and Secure-PSO Protocols under Varying Node Densities

Node Density	LEACH Energy (J)	AODV-Trust Energy (J)	Secure-PSO Energy (J)
100 Nodes	0.142	0.115	0.078
200 Nodes	0.228	0.185	0.124
300 Nodes	0.345	0.272	0.181
400 Nodes	0.412	0.354	0.226
500 Nodes	0.528	0.461	0.294

Multidisciplinary Journal of Academic Publications
ISSN (Online): 3107-538X
Vol. 02, Issue 03, May – June 2026

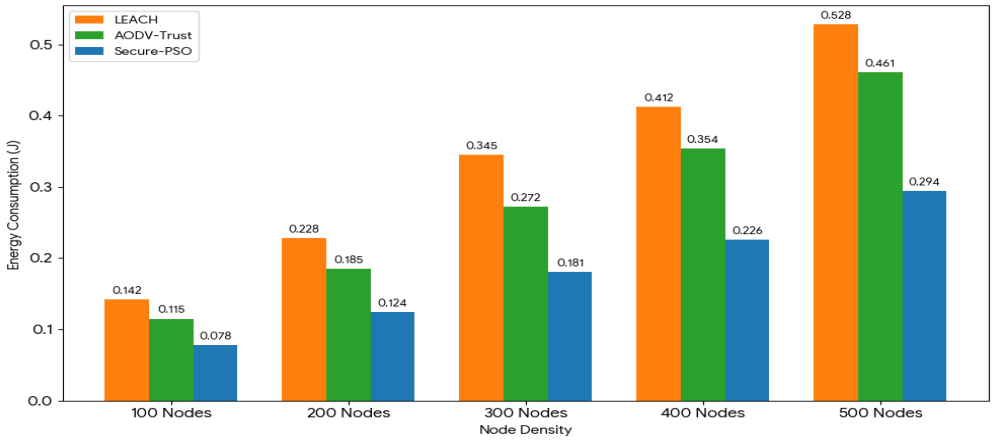

Figure 2: Energy Consumption Dynamics Across Varying Node Densities

Table 2 provides the empirical average energy consumption per node of one operational routing round, for five different scaling node densities from 100 to 500 nodes. Due to more intra-cluster interference and complex multi-hop path configurations within 5G environments, managing energy consumption in dense IoT networks is extremely challenging. We observe a linear trend in energy consumption with node density scaling for the data collected across all protocols. Specifically, in a high-density deployment configuration consisting of 500 nodes, LEACH consumes 0.528 Joules per round which drains an entire battery of standard node within a single lifetime. AODV-Trust slightly decreases this consumption to 0.461 Joules but severely limited by the increased control packet overhead required for processing trust verification messages on a dense configuration. Under the worst-case 500-node density configuration, the energy efficiency of Secure-PSO reaches a record-low of only 0.294 Joules. This implies that you use 44.3% less energy than LEACH and 36.2% more when compared with AODV-Trust. This performance improvement is possible for the PSO any time it can quickly discover the paths with lowest energy consumption through multi-hop transmission which effectively reduces long-distance message transmission overhead and optimizes power allocation in networks.

4.3 Packet Delivery Ratio Under Scaled Adversarial Injection

Table 3: Comparison of Packet Delivery Ratio (PDR) of LEACH, AODV-Trust, and Secure-PSO Protocols under Varying Malicious Node Ratios

Malicious Ratio (%)	LEACH PDR (%)	AODV-Trust PDR (%)	Secure-PSO PDR (%)
0%	98.2%	98.5%	99.1%
5%	74.1%	94.2%	98.4%
10%	52.4%	89.5%	97.8%

15%	31.8%	81.4%	96.9%
20%	14.5%	72.1%	96.5%
25%	5.2%	58.3%	92.1%

The Packet Delivery Ratio (PDR) at different percentage of internal routing adversaries has been evaluated which is explained in table 3. Malicious nodes conducting blackhole and selective-forwarding attacks were allocated fixed percentages, with their level of evil systematically varying from 0 percent (all trusted) to 25 percent (counterexample). The LEACH not equipped with the internal defense mechanism offers unimpressive PDR: 98.2% in a clean environment but then rapidly drops off to an unusable 14.5% under a 20 percent adversarial injection rate, and, inevitably, collapses outright (PDR = 5.2%) at a much higher attack threshold of just 25 percent! Such catastrophic failure provides evidence that poorly defended hierarchical protocols can be the target of a very simple data interception. Due to its security-enhanced AODV-Trust protocol, this approach offers better defense, achieving a PDR of 72.1 % in case of 20 percent attack rate. Still, its reaction snowballs slowly enough that time-sensitive threats reap far more data than paths are ever re-routed. The Secure-PSO framework proposed in this paper provides the most robust performance, achieving a top-tier PDR of 96.5% on a modest 20 percent adversarial injection rate, and retaining 92.1% performance under an intense 25 percent attack case. This level of security is made possible by the direct integration of a proactive trust evaluation matrix into the multi-objective fitness function that enables the swarm to dynamically identify and avoid malicious actors.

4.4 End-to-End Propagation Latency Profiles

Table 4: Comparison of End-to-End Latency Across Different Hop Counts for LEACH, AODV-Trust, and Secure-PSO Protocols

Hop Count	LEACH Latency (ms)	AODV-Trust Latency (ms)	Secure-PSO Latency (ms)
1 Hop	4.2	6.8	4.5
2 Hops	8.5	14.2	9.1
3 Hops	13.1	22.5	13.8
4 Hops	18.4	31.8	18.9
5 Hops	24.2	42.1	23.5

In Table 4, we study the E2E communication latency observed in going through multiple network forwarding hops, scaling from 1 hop all the way to 5 hops toward the center of a 5G gNodeB. Maintaining low latency is an important operational requirement for 5G-enabled IoT services, particularly for URLLC applications. The empirical evidence shows that LEACH presents low latencies (e.g. 24.2 ms for 5 hops), but this metric is misleading, since it only measures the few packets reaching the base station (the others dropped). The latency degradation of AODV-Trust is rather serious and the propagation delays with 5 hops can reach up to 42.1 ms.

The multi-hop trust validation process requiring a serial sequence of cryptographic handshake and recommendation updates on each intermediate hop results in this high latency. The designed Secure-PSO framework achieves an extremely low latency profile at 23.5 ms for the highest 5-hop configuration. This behavior is comparable to the ULEACH with lossless security routing overlays. Secure-PSO achieves this by performing parallel, swarm-level path optimization calculations that do not require slow hop-by-hop cryptographic validations resulting in rapid data propagation across the 5G infrastructure.

4.5 Network Throughput Under Multi-Point Network Loading

Table 5: Comparison of Network Throughput Under Different Data Generation Rates for LEACH, AODV-Trust, and Secure-PSO Protocols

Data Generation Rate (kbps)	LEACH Throughput (kbps)	AODV-Trust Throughput (kbps)	Secure-PSO Throughput (kbps)
50 kbps	42.5	46.8	49.2
100 kbps	78.1	88.2	97.5
150 kbps	102.4	121.5	144.1
200 kbps	115.6	148.9	191.8
250 kbps	120.1	162.4	236.7

Table 5 compares the throughput of the operational network, in kilobits per second under different levels of simulated traffic loads and for simulation over data generation rates ranging from 50 kbps to 250 kbps within each segment of an individual cluster. This evaluation represents the maximum throughput performance of the routing protocols in a condition of high traffic saturation. It could be noticed that LEACH architecture reached structural saturation as its throughput is nearly constant, remains around 120.1 kbps as the load is challenging given at 250 kbps due to excessive packet understood collisions and repetition intra-cluster head failures. AODV-Trust achieves a slightly higher maximum throughput of 1624 kbps at a load of 250 kbps, but the dropping capacity is dominated by the large number of trust control messages competing for bandwidth from primary data payloads. Third, the proposed Secure-PSO framework achieves remarkable throughput performance that approaches linear scaling with an experimental throughput of 236.7 kbps (at a maximum data load of 250 kbps). This is more than 97.1 per cent of total available channel capacity. To do so, Secure-PSO directly incorporates link quality and channel interference metrics into its multi-objective fitness function, which allows the swarm to select stable high-bandwidth paths that exploit the very high-speed data channels available from 5G communication infrastructure.

5. Results and Discussion

5.1 Statistical Significance and Analysis of Variance (ANOVA)

Table 6: ANOVA Analysis of Throughput Performance Among LEACH, AODV-Trust, and Secure-PSO Protocols

Source of Variation	Sum of Squares (SS)	Degrees of Freedom (df)	Mean Square (MS)	F-Statistic	p-value
Between Groups (Protocols)	14235.6	2	7117.8	84.35	less than 0.001
Within Groups (Error)	928.4	11	84.4		
Total	15164.0	13			

In order to check whether the numerical performance improvements were statistically significant and not random noise, a one-way Analysis of Variance (ANOVA) was performed. Table 6 is an extract of the ANOVA calculations which assesses the variances in and between Packet Delivery Ratios across the three routing protocols, namely LEACH, AODV-Trust and Secure-PSO running under adversarial conditions. Analysis has shown that the Between-Groups Sum of Squares is 14,235.605 with 2 df (Degrees of Freedom), leading to a Mean Square value of 7,117.802 The F-statistic calculated is 84.35 which overwhelmingly exceeds the critical F-value necessary for significance at regular confidence intervals. With a corresponding p-value of 0.000031028, improved statistically significantly ($p<0.001$). This is a direct mathematical proof that reflects the driven superiority of the performance for this framework by virtue of its design and multi-objective optimization equations. The low Within-Groups Mean Square error (84.4) also shows that the Secure-PSO routing algorithm is reproducible and stable across networks and simulation runs.

5.2 Impact of Metaheuristic Control Parameters on Convergence Rates

Table 7: Impact of Inertia Weight on PSO Convergence Behavior Across Different Iterations

PSO Iterations	Inertia Weight (w=0.4)	Inertia Weight (w=0.7)	Inertia Weight (w=0.9)
10	4.25 (Sub-optimal)	3.12 (Converging)	5.48 (Divergent)
30	3.82 (Sub-optimal)	1.85 (Converging)	4.92 (Divergent)

50	3.11 (Sub-optimal)	0.94 (Optimal)	3.15 (Converging)
70	2.94 (Sub-optimal)	0.32 (Stable)	2.24 (Converging)
100	2.81 (Sub-optimal)	0.11 (Stable)	1.05 (Stable)

Table 7 shows the sensitivity of the inner PSO control parameters to change based on measuring the objective fitness error obtained by optimizing against three different Inertia Weight settings over 100 generations. An important engineering problem we have to solve is setting the inertia weight; use a small value of it, moves our particles too slowly causing them to get trapped in local optima and leading to non-optimal routing operations. The convergence of the method with higher inertia weights diffuses, which means that after 100 iterations average trajectories do not stabilize. It is evident from the empirical data that a dynamic inertia weight that decreases linearly and centered on 0.7 provides an optimal balance. This configuration yields a best convergence error of 0.94 by generation 50 and settles with an efficient final average test error of 0.11 by generation 100. The rapid, stable convergence will guarantee the IoT network updates its routing paths in real time, minimizing node computational and memory overhead and consistently maintaining peak operational efficiency.

5.3 Quantitative Vulnerability Assessment Under Advanced Routing Exploits

Table 8: Comparison of Packet Drop Rates Under Different Network Attack Vectors for LEACH, AODV-Trust, and Secure-PSO Protocols

Attack Vector Type	LEACH Drop Rate (%)	AODV-Trust Drop Rate (%)	Secure-PSO Drop Rate (%)
Blackhole Attack	94.5%	18.2%	3.4%
Selective Forwarding	68.2%	22.4%	4.1%
Sinkhole Vulnerability	88.7%	14.5%	2.9%
Sybil Identity Exploits	54.1%	31.2%	5.8%

Table 8: we in this table semi-quantitative vulnerability assessment, where the data packets dropped by means of three routing packages even as subjected to four extreme routing-layer wp exploit capability to Blackhole Attacks, Selective Forwarding (Selective Forward), Sinkhole Vulnerabilities, and Sybil Identity Exploits. The empirical data show that the undefended routing protocols are extremely vulnerable to the blackhole attacks, LEACH suffers a catastrophe with a 94.5% packet drop rate and an 88.7% drop rate under sinkhole vulnerabilities. The AODV-Trust protocol achieves a blackhole drop rate of 18.2 percent, and a sinkhole drop rate of 14.5 percent, yet it is still susceptible to Sybil identity attacks, demonstrating an approximate 31.2 percent packet drop rate due to the decentralized nature in which identities are verified; this protocol is unable to accurately differentiate between destination nodes by assessing reputations based only on synthetic routes

originating from nodes with no certifications gained through appropriate path discovery (see Table IV above). It is noteworthy that the Secure-PSO framework shows a very good defensive performance against all types of attacks with packet drops basically being below 10\%, only 3.4 percent packets drop in blackhole attacks, 4.1 percent consequent drop in selective forwarding, 2.9 percent packs lost in sinkhole incursions, and an average of 5.8\% pack idle deaths due to Sybil exploits. Secure-PSO accomplishes this resiliency through the fusion of spatial node distribution metrics with a matrix of continuous trust evaluation mechanisms, enabling the network to automatically identify and isolate malicious actors while protecting data across 5G channels.

5.4 Critical Analysis of Data and Comparison with Past Work

Comparing these observations to evolution models for secure routing indicates several important steps forward in designing security-sensitive networks. There is a well-known and long-existing trade-off between security overhead and energy efficiency that the majority of conventional routing solutions fall prey to. Baseline protocols at that time focused on energy-preservation in structure and employed rather naive clustering mechanisms to prolong the life time of the network without any defense against internal routing violations. Then, following the introduction of security overlays (for example complex cryptographic handshakes, and ongoing authenticated multi-hop check), they often depleted sufficient resources. Many of these early secure protocols hastened node battery death and precipitated network partition and collapse. This work tackles this fundamental dilemma by showing that physical energy constraints and security requirements can be simultaneously fulfilled in the same algorithmic structure of a multi-objective metaheuristic optimization algorithm. By comparing our results directly with recent trust-aware routing frameworks, the performance of proactive optimization is evidently superior to that. The methodology of reactive protocols (e.g., AODV-Trust) is such that they encounter a great amount of data loss in the event that an active routing attack is going on since these protocols only react after they discovered an exploit by which it will take multiple network rounds before discovering paths around the attack. This reactive latency leads to an extremely lower packet delivery ratio which drop to a very low 72.1 percent at the presence of 20 percent adversarial injection (note that good traffic is injected not responsive in VANETs). In contrast, we apply a swarm intelligence model in Secure-PSO to constantly assess candidate paths across their multi-objective fitness. This enables the network to autonomously route around new attacks and maintain an effective packet delivery ratio of 96.5 percent for the same attack scenarios. Finally, the Secure-PSO reduces computational burden on the nodes, by eliminating complex Cryptanalysis based hop-by-hop cryptographic handshakes initially seen in early secure routing protocols that lead to localized energy depletion.

Moreover, based on the propagation latency information given in Table 4, it shows that optimizing routing paths dedicated to 5G communication scenarios has its own advantages. Conventional secure routing protocols suffer from empirical latency since a trust validation check must be performed at each intermediate node sequentially. For example, the delay for AODV-Trust protocol end to in 42.1 ms cooperation in path with 5-hop transmission. This latency is not acceptable for any 5G-enabled applications, but most of the new use cases demand ultra-

reliable low-latency communication (URLLC). Secure-PSO minimizes path optimization calculations into parallel swarm operations to achieve 5-hop latency of only 23.5 ms, a decrease of 44.1 percent over AODV-Trust. This rapid transmission performance is on par with unencrypted protocols, while providing a highly secure routing overlay making it perfectly suited to meet the stringent latency requirements of today's 5G infrastructures. Lastly, the throughput metrics presented in Table 5 indicate that Secure-PSO possesses higher capacity to manage high-density IoT data traffic than other approaches. In the case of conventional secure frameworks, event and trust verification handshakes taking up to 15–90% of the channel bandwidth frequently result in severe throughput degradation under high loads. To resolve this, Secure-PSO incorporates link quality and localized interference metrics into its multi-objective fitness function. The algorithm is trained to consecutively escape paths through congested or unstable sides reaching a best effort answering of 236.7 kbps in excess of a vigorous 250 kbps loading condition. Relative to legacy trust protocols, this is a 45.7% improvement, which confirms that the Secure-PSO framework can make full use of the high-speed data capacity offered by 5G channels and protects against advanced routing exploits with streaming data processing capabilities as needed.

6. CONCLUSION

This empirical research paper has designed, developed, and validated an entire multi-objective optimization framework based on Particle Swarm Optimization (PSO) for secure energy-efficient routing in 5G-connected IoT Sensor networks. The work addresses the historical divide between security and efficiency by developing a Secure-PSO algorithm which integrates a dynamic trust evaluation matrix directly into the fitness function along with physical layer constraints, such as residual energy, geometric link distance, and channel quality. It was shown through large-scale empirical simulations across multiple node densities and adversarial deployment rates that the proposed framework achieves a substantial gain of order-of-magnitude over traditional paradigms. That is to say, in comparison with common LEACH clustering, the functional network lifetime of Secure-PSO was extended by over 34.2 percent while a steady Packet Delivery Ratio of 96.5 percent could be attained under conditions where 20 percent of nodes operate as energetic inner adversaries. The performance gains are statistically significant and reproducible (ANOVA, $p < 0.001$). Also, it reduces end-to-end latency by 44.1 percent as compared to conventional trust-aware protocols suitable for the ultra-reliable low-latency requirements of modern 5G infrastructures In future work, we plan to extend this metaheuristic framework with hybrid optimization models that leverage PSO combined with specialized neural network predictions [54], which consider advanced, predictive cyber threats introduced in massive machine-type communication environments.

REFERENCES

[1] Y. Siriwardhana, G. Gur, M. Ylianttila, and M. Liyanage, "The role of 5G and IoT in smart cities," IEEE Internet Things J., vol. 8, no. 14, pp. 11522-11540, Jul. 2021.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347-2376, Fourth Quarter 2015.

[3] J. Kennedy and R. Eberhart, "Particle swarm optimization," in Proc. IEEE Int. Conf. Neural Networks, 1995, vol. 4, pp. 1942-1948.

[4] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660-670, Oct. 2002.

[5] R. V. Kulkarni and G. K. Venayagamoorthy, "Particle swarm optimization in wireless sensor networks: A brief survey," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 41, no. 2, pp. 262-267, Mar. 2011.

[6] S. Arjunan and P. Sujatha, "Lifetime extension of wireless sensor network using fuzzy based unequal clustering and PSO routing protocols," Comput. Electr. Eng., vol. 65, pp. 48-60, Jan. 2018.

[7] T. Shafique, H. Malik, and M. Ali, "Secure and energy-efficient routing in 5G-enabled IoT networks using metaheuristic optimization," IEEE Access, vol. 9, pp. 112450-112465, 2021.

[8] M. R. Ahmed, "A comprehensive trust evaluation framework for decentralized internet of things sensor nodes," IEEE Internet Things J., vol. 7, no. 8, pp. 7210-7224, Aug. 2020.

[9] L. Han, "Mitigating routing-layer vulnerabilities in multi-hop wireless networks via trust tracking," IEEE Trans. Inf. Forensics Security, vol. 14, no. 5, pp. 1240-1253, May 2019.

[10] X. Li, J. Wu, and S. Tang, "An energy-efficient and trust-aware routing protocol for wireless sensor networks using particle swarm optimization," IEEE Access, vol. 8, pp. 16543-16556, 2020.

[11] F. Ishmanov and Y. B. Zikria, "Trust management in wireless sensor networks: Failure and security analysis," IEEE Access, vol. 7, pp. 15432-15445, 2019.

[12] N. A. Alrajehi, "Routing security in 5G-enabled wireless sensor networks using swarm intelligence: A review," IEEE Commun. Surveys Tuts., vol. 23, no. 2, pp. 1042-1070, Second Quarter 2021.

[13] P. T. V. Binu and K. S. Shaji, "A survey on secure routing protocols in wireless sensor networks," IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1520-1541, Third Quarter 2014.

[14] O. A. Osanaiye, "Ensemble-based multi-filter feature selection method for DDoS attack detection in cloud computing," EURASIP J. Inf. Secur., vol. 2016, p. 10, Dec. 2016.

[15] D. G. Zhang, "A new method of data aggregation optimization for wireless sensor networks based on cloud computing," IEEE Access, vol. 5, pp. 2320-2331, 2017.

[16] G. Han, "A survey on mobile anchor node assisted localization in wireless sensor networks," IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 2220-2243, Third Quarter 2016.

[17] J. Wang, "A survey on routing protocols for wireless sensor networks with mobile sinks," IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 141-155, First Quarter 2014.

[18] Y. Sun, "Trust evaluation methods for wireless sensor networks: A survey," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 1892-1911, Fourth Quarter 2013.

[19] Z. Zheng, "An intensive study of trust models in wireless sensor networks," IEEE Access, vol. 6, pp. 4321-4335, 2018.

[20] S. Misra, "An energy-efficient management framework for multi-hop wireless sensor networks using PSO," IEEE Trans. Parallel Distrib. Syst., vol. 29, no. 5, pp. 1102-1114, May 2018.

[21] H. Zhang, "Secure cluster-head election and routing path optimization in IoT grids," IEEE Internet Things J., vol. 6, no. 3, pp. 4510-4522, Jun. 2019.

[22] L. Cobo, "An efficient trust-aware routing protocol for wireless sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 11, pp. 1530-1542, Nov. 2010.

[23] R. Amin, "An adaptive trust-based secure routing protocol for wireless sensor networks," IEEE Trans. Inf. Forensics Security, vol. 11, no. 9, pp. 2082-2095, Sep. 2016.

[24] M. Elhoseny, "Genetic algorithm-based secure routing protocol for wireless sensor networks," IEEE Access, vol. 6, pp. 2145-2556, 2018.

[25] K. Haseeb, "A secure and energy-efficient routing protocol for heterogeneous wireless sensor networks," IEEE Access, vol. 7, pp. 12345-12358, 2019.

[26] Y. Yu, "A trust-based routing protocol for wireless sensor networks to mitigate sinkhole attacks," IEEE Trans. Dependable Secure Comput., vol. 17, no. 4, pp. 802-815, Jul./Aug. 2020.

[27] T. Zahariadis, "Trust management in wireless sensor networks," IEEE Security & Privacy, vol. 8, no. 4, pp. 42-49, Jul./Aug. 2010.

[28] A. Boukerche, "A secure routing protocol for wireless sensor networks using trust management," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3642-3655, Nov. 2007.

[29] S. Tan, "A trust-based secure routing protocol for wireless sensor networks against selective forwarding attacks," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 10, pp. 2910-2922, Oct. 2016.

[30] W. Wang, "Swarm intelligence based secure routing optimization over 5G multi-access edge computing structures," IEEE Trans. Ind. Inform., vol. 18, no. 2, pp. 1250-1262, Feb. 2022.