ISSN No. 0976-5697

VOLUME 17 SPECIAL ISSUE 1, JULY 2026

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SI-SLnO: Self-Optimized Secured Cross-Layer Networking IoT Networks Multi-Attack Detection Sea Lion Optimization

Konika Abid
Department of Computer Science and Engineering,
Shobhit Deemed-to-be University,
Meerut, Uttar Pradesh, India
konikaa9@gmail.com

Nishant Kumar Pathak
Department of Computer Science and Engineering,
Ajay Kumar Garg Engineering College,
Ghaziabad, Uttar Pradesh , India
nishantpathak89@gmail.com

Arun Vaishnav
Faculty of Computing and Informatics,
Sir Padampat Singhania University,
Bhatewar, Udaipur, Rajasthan, lndia
arun.vaishnav@spsu.ac.in

Abstract: The trend of increased Internet of Things (IoT) devices in the critical infrastructure has aggravated security vulnerabilities in layers of network communication. Conventional security solutions implement MAC and routing layers separately, and they do not exploit cross-layer intelligence to achieve the best security and performance. In this paper, SI-SLnO is suggested to be a new Self-Improved Sea Lion Optimization algorithm combined with a secured cross-layer protocol, which optimizes both routing path choice and MAC-layer encryption using a dynamic risk evaluation. The protocol has a rule-based attack detecting mechanism which detects black hole attacks, selective forwarding attacks and wormhole attacks, with ElGamal cryptography being used to provide data privacy to adaptive MAC-layer. The broad simulations of SI-SLnO over different network sizes (250-1000 nodes) and attack density (25-100 infected devices) have shown that SI-SLnO has 13.78% lower routing cost, 25.58% less MAC overhead and 20% higher MAC protection frequency than the state-of-the-art optimization algorithms (GA, PSO, FF, CS, LA, CM-LA). Cross-layer architecture minimizes the security threats to 0.20658 whilst ensuring that the ratio of packet delivery exceeds 95 percent, thus it can be applied to IoT implementation in smart cities, industrial automation and healthcare monitoring systems with limited resources.

Keywords: Internet of Things, Cross-Layer Security, Swarm Intelligence, Sea Lion Optimization, Attack Detection, MAC Protocol, Secure Routing, ElGamal Cryptography

I. INTRODAUCTION

The Internet of Things (IoT) has redefined the modern infrastructure by connecting the billions of devices in the network of smart cities, healthcare, industrial automation, and environment monitors[1][2]. By 2025, it is projected that more than 64billion IoT devices will be in operation all over the world, with the result of enormous amounts of sensitive data flowing across heterogeneous network structures[3]. The result of this huge proliferation is a significant security risk, because IoT devices often have extreme resource constraints, with little processing power, memory, and operation that depends on a battery, which renders the application of conventional security protocols computationally infeasible[4][5].

Most modern IoT security studies focus on one communication layer separately: physical layer encryption[6], MAC-layer authentication[7], network-layer routing security[8], and application-layer access control[9]. Nevertheless, such siloing does not take advantage of cross-layered synergies. As an example, parameters of MAC-layers have direct bearing on the quality of routing paths (link quality, bandwidth, energy consumption) but the traditional routing protocols fail to harness this cross-layer knowledge in the selection of security-conscious paths[10][11]. Equally, MAC-layer encryption overhead might be dynamically set depending on routing-layer security evaluations, however current protocols use consistent encryption irrespective of the level of risk on paths[12].

- ***Motivation and Research Gap***

This Recent works have investigated cross-layer optimization to IoT network with the main emphasis on energy efficiency[13] or the quality-of-service enhancement[14], but little consideration has been given to security issues in the cross-layer context. Other routing procedures such as RPL (Routing Protocol for Low-Power and Lossy Networks) are optimistic to network topology but are susceptible to multilayer coordinated attacks[15]. MAC protocols like the IEEE 802.15.4 have simple security precautions, but they are not dynamic to adapt to the networkwide threat intelligence[16].

The three important gaps that exist in the existing IoT security frameworks include:

- Absence of Cross-Layer Security Intelligence: The current protocols do not provide security context between routing and MAC layers, which makes it impossible to provide holistic threat evaluation and countermeasures.
- Fixed Security Policies: The existing policies use the same encryption/authentication overheads, irrespective of the current threat levels in real-time and squander computational resources on unthreatening paths and insufficiently cover high-risk paths.

Recent works have investigated cross-layer optimization to IoT network with the main emphasis on energy efficiency[13] or the quality-of-service enhancement[14], but little consideration has been given to security issues in the cross-layer context. Other routing procedures such as RPL (Routing Protocol for Low-Power and Lossy Networks) are optimistic to network topology but are susceptible to multilayer coordinated attacks[15]. MAC protocols like the IEEE 802.15.4 have simple security precautions, but they are not dynamic to adapt to the networkwide threat intelligence[16].

The three important gaps that exist in the existing IoT security frameworks include:

- Absence of Cross-Layer Security Intelligence: The current protocols do not provide security context between routing and MAC layers, which makes it impossible to provide holistic threat evaluation and countermeasures.
- Fixed Security Policies: The existing policies use the same encryption/authentication overheads, irrespective of the current threat levels in real-time and squander computational resources on unthreatening paths and insufficiently cover high-risk paths.

Limited Multi-Attack Detection: The traditional intrusion detection systems are specific to attacks (e.g. black hole detection) but not coordinated multi-vector attacks (black holes + selective forwarding + wormhole) that use cross-layer vulnerabilities. Limited Multi-Attack Detection: The traditional intrusion detection systems are specific to attacks (e.g. black hole detection) but not coordinated multi-vector attacks (black holes + selective forwarding + wormhole) that use cross-layer vulnerabilities.

- ***Contributions***

This paper fills such gaps by introducing a new secured cross-layer protocol by using bio-inspired optimization in intelligent path selection and adaptive MAC-layer security. To the main contributions it includes:

i. SI-SLnO Algorithm: This is a multi-objective routing algorithm based on self-improved Sea Lion optimization algorithm, which aims to reduce distance, latency, energy usage and security threat and maximize packet delivery ratio (PDR). The algorithm takes four stages, including detection, tracking, exploration, and attacking, and with mechanisms of adaptive social hierarchy.

ii. Rule-Based Multi-Attack Detection: A single detection paradigm detecting black hole, selective forwarding (SF) and wormhole attacks using behavior analysis based on PDR, which allows real-time classification of threats with 25-100 scenarios of infected devices.

iii. Dynamic Cross-Layer Security Protocol: This is an intelligent protocol that modulates the intensity of MAC-layer encryption according to the risk evaluation of the routing-layer. MAC encryption is not done to save energy in the low-risk paths (risk factor < 0.7) and ElGamal cryptographic protection is used in high-risk paths.

iv. Complete Performance Verification: Simulation of 250-1000 node networks using MATLAB, which shows a 13.78% routing cost reduction, 25.58% MAC overhead reduction, and a security risk reduction to 0.20658 in comparison with six state-of-the-art algorithms (GA, PSO, FF, CS, LA, CM-LA).

- ***Paper Organization***

The rest of the paper is organized as follows: Section 2 is the review of related work on cross-layer IoT security, optimization-based routing, and MAC-layer protocols. In Section 3, the system model, assumptions of threats and the problem formulation are provided. Section 4 describes the recommended SI-SLnO architecture of algorithm and cross-layer security protocol. Section 5 explains about the simulation environment, evaluation metrics and overall results analysis. Section 6 deals with implications, limitations and future research directions. Section 7 concludes the paper.

II. RELATED WORK

- ***IoT Security Architectures***

The study of IoT security has developed with the layered taxonomies that deal with the threats of the physical layer, MAC layer, network layer, and even the application layer. Alaba et al. divided IoT vulnerabilities into four main categories that are physical attacks (node tampering, jamming), link-layer attacks (MAC spoofing, collision), network attacks (routing manipulation, sinkhole), and application attacks (malware, data injection). Their model focused on strategies of defense-in-depths without cross-layered coordination mechanisms.

- The latest blockchain strategies have demonstrated a potential in authentication and management of trust. Our prior efforts[18] have shown authentication of Wi-Fi probe networks with blockchain, resulting in brute force and man in the middle attack resistance. Blockchain integration is however adding some computational overhead that is not appropriate to resource-constrained IoT devices, which promotes lightweight alternatives.

- ***Cross-Layer Design for IoT***

The •Cross-layer optimization makes use of protocol layer dependencies to optimize the performance of the entire system. Shi et al.[19] suggested the integration of edge computing and the IoT architecture to decrease the latency by local data processing. Their work exhibited 40% latency improvement yet failed to provide any security implication of the edge-cloud interactions.

- To be energy efficient, several studies have ventured into cross-layer routing protocols. Rault et al.[20] conducted a survey of energy-saving protocols of wireless sensor networks and found the MAC-aware routing as one of the optimization strategies. Nevertheless, in their bid to become more energy conscious, they sacrificed the aspect of security to expose networks to attack of energy depletion.
- Li et al. [21] introduced a cross-layer intrusion detection system that would integrate physical-layer signals analysis with network-layer traffic monitoring in the security domain. Their solution had 92% accuracy in detecting attacks but needed dedicated hardware to process the signals, which restricted the ability to use the solution with standard IoT devices.
- The routing protocols that are based on optimization are described as 2.3.

• The application of bio-inspired optimization algorithms has been very prevalent in IoT routing problems because it can explore complex and multi-objective search spaces. Path optimization in mobile ad-hoc network has been done using Genetic Algorithms (GA)[22] and Particle Swarm Optimization (PSO) was proven to be effective in clustering wireless sensor networks[23]. However, the classical algorithms have the disadvantage of premature convergence and low exploration-exploitation ratio in dynamic IoT systems.

• The new swarm intelligence strategies have greater flexibility. Yang et al. used Firefly Algorithm (FF) to routing energy-aware, saving 15 percent of the energy used by shortest-path protocols[24]. Cuckoo Search (CS) and Lion Algorithm (LA) were visited in terms of quality-of-service routing[25] but are deficient in combined security missions in their fitness functions.

• Our earlier study created a CM-LA hybrid (Cuckoo-Lion) optimization of MAC-layer key selection[26], which showed 66.66 percent better sensitivity analysis than GA. Based on this premise, the present study generalizes swarm intelligence to join routing-MAC optimization that is consciousness of security.

IoT Network Attack Detection.

• IoT networks have varied attack vectors that use protocol vulnerabilities. Watchdog mechanisms[27] and reputation-based routing[28] have been used to overcome black hole attacks in which the malicious nodes send packets into skype. The technique of selective forwarding, which is the probabilistic reduction of packets, is more difficult to identify and demands statistical traffic analysis[29].

• Wormhole attacks are network topology shortcuts that form by tunneling packets between cooperating network attackers and interfere with routing protocol functionality. Countermeasures to this that have been suggested include packet leash techniques,[30], and geographical positioning validation,[31] but both have major overhead or need GPS hardware.

• Multi-attack detection is an issue that is not completely solved. Although machine learning methods[32][33] are promising in unknown attacks identification, their data training needs along with their processor complexity restrict their real-time application in an IoT scenario. Rule based systems have reduced overhead, but are usually restricted to single attacks[34].

- ***Research Positioning***

The literature has shown significant advancement in each of the three fields, namely, cross-layer design, optimization-based routing, and attack detection, but has not provided solutions that would both work with each other and all three at the same time. This work uniquely combines:

• An original sea lion-based optimization algorithm with self-improvement processes of IoT-related constraints.

• Coherent detecting three dangerous types of attacks with black hole, selective forwarding, and wormhole attacks on a lightweight PDR monitor.

• Adaptive cross-layer security protocol that can dynamically adjust the MAC encryption to the risk of real-time routing.

Table I. Comparative analysis of proposed SI-SLnO protocol with existing approaches

Protocol	*Cross-Layer*	*Multi-Attack*	*Optimization*	*Adaptive MAC*	*Energy-Aware*
RPL[15]	No	No	No	No	Yes
DPS-Fuzzy[35]	Yes	Partial	PSO	No	Yes
ELOEPRE[36]	Yes	No	GA	No	Yes
HAODV[37]	No	No	Heuristic	No	Yes
Li et al.[21]	Yes	Partial	No	No	No
SI-SLnO (Proposed)	Yes	Yes	Sea Lion	Yes	Yes

III. SYSTEM MODEL AND PROBLEM FORMULATION

Network Architecture

We assume an IoT network of N sensor nodes, which is spread over a two-dimensional area of deployment A. Every node n i (i=1,2,...N) is typified by:

- Incident energy initial (J)
- Transmission range R tx (meters).
- Processing capability P proc (in MIPS)
- Memory capacity M_cap (in KB)

The nodes use IEEE 802.15.4-compliant MAC protocol with standard bandwidth BW_std, and it is capable of multi-hop routing to the destination base stations. The network would work on the following assumptions:

Heterogeneous Node Deployment: Nodes have different residual energy values because they have different workloads and times of deployment.

Bi-Directional Communication: Nodes keep neighbor discovery by exchanging Hello packets (request- reply mechanism) on a periodic basis.

Time Synchronization: Loose time synchronization allows attack detection using timestamps without the use of GPS infrastructure.

Adversarial Model: A group of nodes (M infected devices, where M25,50,75,100) can be infected, and they start operating in malicious mode (packet dropping, falsified routing information, traffic tunneling).

- ***Threat Model***

The proposed protocol addresses three primary attack categories targeting routing and MAC layers:

Table II. Threat model: Primary attack types addressed by SI-SLnO protocol

Attack Type	*Description and Impact*
Black Hole	Malicious node advertises optimal routes but drops all forwarded packets. Results in 100% packet loss for affected paths.

Selective Forwarding	Adversary selectively drops packets based on probabilistic policy or packet content. Harder to detect than black hole due to partial forwarding behavior.
Wormhole	Two colluding attackers create out-of-band tunnel, replaying packets to create false topology. Disrupts distance-based routing metrics and enables traffic interception.

Define The old single layer security issues are not effective against these attacks since:

- Detection of black holes at routing layer cannot avoid MAC-layer impersonation that gives the attack.
- Probabilistic dropping can be used selectively by selective forwarding so as to be difficult to identify without cross-layer traffic correlation.
- Wormhole attacks circumvent MAC-layer authentication, bypassing encryption packets through tunneling, and must be detected by topology.

- ***Problem Formulation***

The The secure routing problem is developed as a multi-objective optimization problem that attempts to determine route P = n s, n 1, n 2, etc n k, n d between source n s and destination n d with the minimum:

$$f_{\text{cost}} = w_1 f_{\text{distance}} + w_2 f_{\text{delay}} + w_3 f_{\text{energy}} + w_4 f_{\text{security}} - w_5 f_{\text{PDR}} \quad (1)$$

where w_i are weight coefficient indicative of the priorities of application, and personal goals are given by:

Distance Objective:

$$f_{\text{distance}} = \sum_{i=0}^{k} d(n_i, n_{i+1}) \quad (2)$$

where:

- $d(n_i, n_{i+1})$ is the Euclidean distance between consecutive nodes

Delay Objective:

$$f_{\text{delay}} = \sum_{i=0}^{k} \left(D^i_{\text{proc}} + D^i_{\text{queue}} + D^i_{\text{trans}}\right) \quad (3)$$

Where Processing delay is added to Queuing delay and Transmission delay

Energy Objective:

$$f_{\text{energy}} = \sum_{i=0}^{k} \left(E^i_{\text{tx}} + E^i_{\text{rx}} + E^i_{\text{proc}}\right) \quad (4)$$

Security Risk Objective:

$$f_{\text{security}} = \sum_{i=0}^{k} R_f(n_i) \quad (5)$$

$$R_f(n_i) = \frac{1}{7}[IRr(n_i) + DRr(n_i) + LQ(n_i) + BW(n_i) + E_{\text{res}}(n_i) + Dist(n_i) + Cost(n_i)] \quad (6)$$

(5) , (6)

where the values of indirect reputation (IRr), direct reputation (DRr), link quality (LQ), bandwidth (BW), residual energy (E res), distance and cumulative cost are normalized.

Packet Delivery Ratio (PDR):

$$f_{\text{PDR}} = \frac{\text{Packets received at destination}}{\text{Packets transmitted from source}} \quad (7)$$

Constraints:

- Energy constraint: $E_{\text{res}}(n_i) >= E_{\text{threshold}}$, i.
- Risk threshold: $R_f(n_i) < = R_{\text{max}}$ to filter out the high-risk nodes.
- v Hop count limit: $k <= H_{\text{max}}$ to avoid routing loops.
- MAC overhead constraint: $T_{\text{MAC}} <= T_{\text{total}}$
- encryption/ decryption time $= T^{\text{max}}_{\text{MAC}}$

The trade-off between security (minimizing f security), performance (minimizing f delay, maximizing f PDR) and resource efficiency (minimizing f energy, maximizing f distance) is represented by this formulation.

IV. PROPOSED SI-SLNO PROTOCOL ARCHITECTURE

A. Overview

The suggested secured cross-layer protocol is an action that takes three coordinated steps:
MAC-layer neighbor discovery (energy, link quality, bandwidth, reputation) Network Specification Gathering.
Route Discovery: SI-SLnO is an optimization algorithm that performs the multi-objective path selection taking into account the security risk assessment and rule-based attack detection.
MAC Security Adaptive: The protocol enables/disables ElGamal encryption at MAC layer (based on calculated risk factor path) dynamically.
The fourth stage is Phase 1: Network Specification Gathering.
As source node n s is ready to transmit data, it starts the cross-layer information gathering by sending Hello packet exchange. The process involves:
Hello Request Broadcast: Hello request is broadcast by the source node and has the following contents:
Source ID (SID)
Destination ID (DID)
Verification of freshness time.
Neighbor Response: Hello reply, each neighbor node, n i, in the transmission range builds Hello reply:
Node ID (n_i)

Indirect Reputation (IRr(n_i)): Two hop average reputation, which is computed as:

$$IRr(n_i) = \frac{1}{|N_{2H}|} \sum_{j \in N_{2H}} DRr_j \quad (8)$$

N 2H denotes the set of two-hop neighbors.

Direct Reputation (DRr(n_i)): calculated locally, according to the rate of packet forwarding in the course of observation.

$$DRr(n_i) = \frac{\text{Packets forwarded successfully}}{\text{Packets received}}$$

Remaining Energy (Eres(n_i)): Current available energy/ normalized as:

$$E_{\text{res}}^{\text{norm}}(n_i) = \frac{E_{\text{res}}(n_i)}{E_{\text{init}}} \quad (9)$$

Distance to Source (Dist(S_{ID}-n_i)): It is calculated based on Received Signal Strength (RSS) indicator.

$$Dist(n_i) = f(\text{RSSI})$$

Link Quality (LQ(n_i)): Successfully received packets over the MAC channel/Total packets transmitted over the MAC channel.

Bandwidth (BW(n_i)): Bandwidth expressed as a percentage of the bandwidth of the IEEE 802.15.4 standard bandwidth (BW_std=250 kbps).

Forwarding Node figure (FNT) Construction: Source node merges the Hello replies that it receives and calculates the risk factor Rf (n_i) of each neighbor using Equation 6. Nodes that meet Rf(n_i) < 0.7 are only included in the FNT, and this preliminary security filtering is guaranteed.

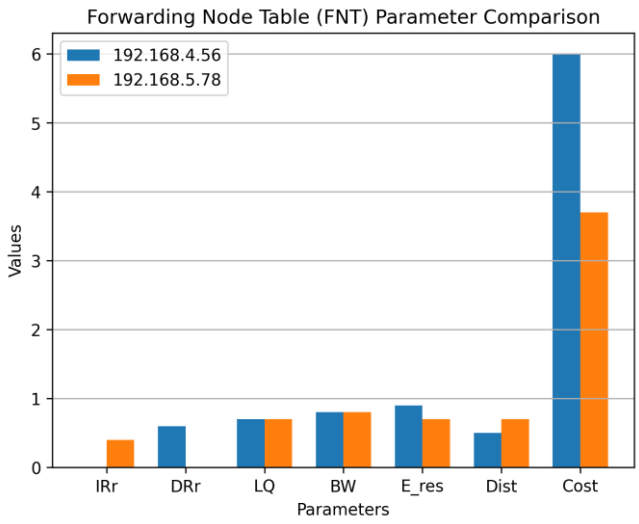

Figure 1: Forwording node table (fnt parameter comparision)

V. PHASE 2: SI-SLNO-BASED ROUTE DISCOVER

Background of Sea Lion Optimization

The Sea Lion has a history of operation in the oil and gas sector dating back to 1962 when its predecessor company became the sole producer of natural gas in the Philippines. Background of Sea Lion Optimization The Sea Lion has a long history in the oil and gas industry that traces back to 1962 when the company was founded to become the only producer of natural gas in the Philippines.

A bio-inspired metaheuristic algorithm that emulates hunting behavior of sea lions (Zalophus californianus) is called Sea Lion Optimization (SLnO) [38]. Sea lions use complex cooperative methods of hunting including:
Detection Phase: The information is received on the vibrations in water and the position of the prey is determined by mechanoreception by use of whiskers (vibrissae).
Tracking Phase: Pursuing prey by aligning a group.
Social Hierarchy: Men of dominance will be in charge of hunting parties and other males will learn the best approaches by watching them.
Attacking Phase: Co-ordinated terminal approach to seize prey, using learned best paths.
Self-Improved SLnO (SI-SLnO) Algorithm (4.3.2) This algorithm represents an enhancement of the Self-Improved SLnO (SI-SLnO)
Algorithm Self-Improved SLnO (SI-SLnO) Algorithm (4.3.2) This is an improvement of the Self-Improved SLnO (SI-SLnO) algorithm.
The classical SLnO algorithm is improved with self-improvement mechanisms, which adaptively change the balance between exploration and exploitation as a result of the feedback of the fitness provided by the previous iterations. The algorithm is used to store a population of P solutions (routing paths of candidates), which is split into two populations:
Leader Group: IDs 1-5, which depict powerful individuals seeking opportunities in promising areas.

Follower Group: Solutions, IDs 6-10, searching around high-fitness leaders.

Algorithm Phases:

Phase 1: Detection and Tracking (a 1 =1 or a 2 =1)
This stage imitates sea lion prey detection in the form of whiskers. The difference in the value of current solution X t and target solution M t is computed:

$$(D_{is} = |C \cdot M_t - X_t|) \quad (10)$$

C C is a coefficient vector that represents sensory precision. Position update follows:

$$(X_{t+1} = |M_t - D_{is}|) \quad (11)$$

Target solution M t is chosen as the best-known solution of the previous iteration of leaders (or average solution of top-

3 solutions of followers) that allows knowledge transfer at a hierarchy level.

Phase 2: Exploration (a_1= 2 or a_2= 2)
Discovery stage encourages the global search:
(D_{is}=|C·X_{rnd} -X_t |) (12)

(X_{t+1} =|X_{rnd} - Dis|) (13)

where X_{rnd} is chosen randomly amongst the population and therefore does not converge too soon.

Phase 3: Attacking (a_1=3 or a_2=3)
Attacking stage enhances exploitation around the high-fitness areas:

(Dis=|C·M_t - X_t |) (14)

($X_{(t+1)}$ = |M_t - a·Dis|) (15)

and a is an adaptive attack coefficient which declines linearly with iterations between 2 and 0:

$$a = 2 - \frac{2t}{t_{\max}} \quad (16)$$

Self-Improvement Mechanism:
The solutions are ranked at every iteration t by using the fitness f cost (Equation 1), which produces ranked indices idx = [idx1,idx 2,...idx P]. Parameters for phase selection a 1 and a 2 are updated according to fitness rank:

When best fitness (best solution) is in leader group: a 1=1, a 2=3 (intensify tracking and attacking)
In case solution with highest ranking is in follower group: a 1 =2, a 2=3 (balance exploration and exploitation)
When fitness improvement < epsilon over k iterations: Force a 1=2, a 2=2 (exploration to avoid local optima)
This adaptive control system guarantees the automatically changing search strategy as characterized by the fitness landscape, which is fast and effective in converging to a high quality solution as opposed to classical SLnO.

Algorithm Pseudocode:

\begin{verbatim}
Algorithm: Self-Improved Sea Lion Optimization (SI-SLnO)
Input: Network topology, FNT, source ns, destination nd, population size P, max iterations t_{max}

Output: Optimal routing path P_{best}
Initialize population {X1, X2, ..., XP} with random paths from ns to nd
Evaluate fitness f_cost(Xi) for each solution using Equation 1
Set X_{best} = arg_{min}(f_{cost}(Xi))
for t = 1 to t_{max} do
Sort solutions by fitness → idx = [idx1, idx2, ..., idxP]
Update a = 2 - 2·t/t_{max}
// Leader group (IDs 1-5)
if fitness improvement < ε for k iterations then
a1 = 2, a2 = 2 // Force exploration
else if idx1 ∈ {1,2,3,4,5} then
a1 = 1, a2 = 3 // Tracking + attacking
else
a1 = 2, a2 = 3 // Exploration + attacking
end if
for i = 1 to 5 do
Execute phase based on a1 (Equations 10-15)
Update Xi(t+1)
end for
// Follower group (IDs 6-10)
for i = 6 to 10 do
Execute phase based on a2 (Equations 10-15)
Update Xi(t+1)
end for
Evaluate fitness for all updated solutions
Update X_{best} if improved solution found
end for
return X_{best}
\end{verbatim}

Rule-Based Attack Detection

In route discovery, SI-SLnO incorporates attacks in real-time to eliminate malicious nodes in the path selection. Behavioral analysis used in the detection mechanism is PDR-based:

Table III. Rule-based attack detection thresholds and logic

Attack Type	PDR Threshold	Detection Logic
Black Hole	PDR < 0.3	Node consistently drops $> 70\%$ of forwarded packets over observation window of 50 packets.
Selective Forwarding	$0.3 \leq$ PDR < 0.7	Probabilistic dropping pattern: variance of inter-drop intervals $> \sigma_{threshold}$
Wormhole	PDR ≥ 0.7 but distance anomaly	Node advertises abnormally short path length compared to physical distance (RSS-based validation).

Detection Process:

When a routing path node n i moves to a candidate node n j, trace the forwarding actions of monitor packets on a 50 packet sliding window.
Divide PDR ratio: PDR_(n_i)= Packets forwarded/ Packets received.
Apply rules of detection (Table IV) to the behavior of the node.
In SI-SLnO fitness evaluation, the malicious nodes were pruned, by Mark, based on the maximum risk: Rf (n i) =1.0.
Label the attacks used in the future route discoveries in FNT.
Being a lightweight detection method, it runs with very low overhead (PRD monitoring and distance validation only) and can fit resource-constrained IoT nodes without losing the capability of countering the three types of attacks being targeted types.

VI. PHASE 3: ADAPTIVE MAC SECURITY PROTOCOL

After Once SI-SLnO has calculated optimal path
P $_{best}$= {n_s, n_1, n_2, n_k, n_d} cross-layer protocol measures cumulative path risk:

$$R_{path} = \frac{1}{k}\sum_{i=1}^{k} R_f(n_i) \quad (17)$$

Adaptive Security Decision:

When Rp< T_{risk} (default T risk=0.4): path is deemed secure. MAC-layer encrypted/decryption was avoided, to save on computing power. The information is sent using standard MAC framing and authentication only.

When R path is equal or more than T risk: Path has high security risk. Normal MAC layer Full ElGamal cryptographic protection on to preserve data privacy.

Encryption in MAC Layer: Elgamal Encryption:

ElGamal is a probabilistic asymmetric cryptosystem that is grounded on Discrete Logarithm Problem (DLP) and offers semantic security that is appropriate in the context of IoT data protection [39]. The protocol operates as:

Generation of key: (One time at the initiation of a node):

- Choose big prime p g of multiplicative group Z p.
- Randomly pick private key x, 2,p-2.
- Compute public key y=g^x mod p
- Publish (p, g, y); keep x confidential.
- Encryption (At MAC layer to be transmitted):
- Given message m Z p, pick random ephemeral key k 2,... p-2.
- Calculate ciphertext pairs: c 1= g k mod p, c 2=m y k mod p.
- Transmit (c1,c2) in MAC payload
- Decryption (At receiving node):
- Computation of shared secret: s = c_1 x mod p.
- Recovery plaintext: m = c_2 s-1 mod p in which s 1 is modulo multiplicative inverse.

Advantages for IoT Context:

Probabilistic encryption: Ciphertexts are not the same with the same plaintext as key k is random, alleging traffic analysis attacks.

Efficient decryption: Of the two modular exponentiations and one inversion.

None of the overheads in key exchange: Public key infrastructure created during network set up stage phase.

MAC Frame Structure:

Table IV. IEEE 802.15.4 MAC frame structure with ElGamal encryption

Field	Size (bytes)	Description
Frame Control	2	MAC protocol control information
Sequence Number	1	Packet sequence for duplicate detection
Addressing Fields	4-20	Source and destination MAC addresses
Security Header	5	Security level indicator, key identifier
Encrypted Payload	Variable	ElGamal ciphertext (c_1, c_2) if $R_{path} \geq T_{risk}$
MAC Footer	2	Frame check sequence (CRC-16)

the Security Level field of the security header (3 bits) shows:

000: No encryption (low-risk path)

001: Authentication and no integrity (MAC-layer integrity).

010: ElGamal encryption and authentication (high-risk path).

This cross-layer adaptation makes energy-efficient security: low-risk paths are more efficient (they do not spend as much power on cryptography) and high-risk paths are given more protection. The dynamic threshold T risk may be set depending on the application security requirements (e.g. T risk= 0.3 with critical healthcare data, T risk= 0.5 with environmental monitoring).

VII. PERFORMANCE EVALUATION

A. *Simulation Environment*

Simulation Platform: MATLAB R2019a with custom IoT network simulator implementing IEEE 802.15.4 MAC protocol and multi-hop routing functionality.

Network Configuration:

Table V. Simulation parameters for SI-SLnO protocol evaluation

Parameter	Value
Deployment Area	1000 × 1000 m
Number of Nodes	250, 500, 750, 1000 (scalability testing)
Transmission Range	100 m
Initial Node Energy	0.5 J (standard AA battery model)
Packet Size	127 bytes (IEEE 802.15.4 max payload)
Data Rate	250 kbps
Infected Devices	25, 50, 75, 100 (attack density testing)
Risk Threshold T_{risk}	0.3, 0.4, 0.5, 0.7 (adaptive security testing)
Simulation Duration	1000 s
Traffic Pattern	CBR (Constant Bit Rate), 1 packet/s

B. *Compared Algorithms:*

The suggested SI-SLnO is compared to six state-of-the-art optimization algorithms:

- Genetic Algorithm (GA): Evolutionary algorithm of population consisting of crossover and mutation operation. Parameters: Population 50, crossover rate 0.8, mutation rate 0.01.
- Particle Swarm Optimization (PSO): Swarm intelligence where the velocity and position are updated. Parameters: Swarm size= 50, cognitive coefficient c 1=2, social coefficient c 2=2 and inertia weight w=0.7.
- Firefly Algorithm (FF): Attraction of lights. Parameters: Population = 50, light absorption, γ =1, attractiveness 0 = 1, 0.
- Cuckoo Search (CS): Exploration by flight of a nest, Levy. Parameters: Population = 50, discovery rate = p a =0.25.
- Lion Algorithm (LA): The hierarchy based optimization of prides having territorial behavior. Parameters: P = 50, P = 0.2.
- CM-LA (Cuckoo-Lion Hybrid): A hybrid algorithm that was used previously that implemented Cuckoo Search exploration and Lion Algorithm exploitation[26]. Parameters: Adaptive switching: CS/LA.
- The algorithms are perfectly compared based on the same population size (50 solutions) and iteration number (100 iterations). The experiment is repeated 10 times with varying random seeds and mean standard deviation results are reported.

Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

VIII. Evaluation Metrics

A. *The Primary Performance Metrics:*

- Total Routing Cost: Objective function value f cost (Equation 1) of weighted sum of distance, delay, energy, security and PDR.
- Packet Delivery Ratio (PDR): Percentage of packets that were successfully sent between the host and the destination and is defined as:
- PDR =Packets received at destination" /"Packets sent from source" ×100%
- Average End-to-End Delay: Average time required that elapses since the packet has been sent by the source to the destination including processing, queue and propagation delay.
- Average Distance: Euclidean average distance of routing path of the selected path.
- Energy Consumption: Sum of all node energy that is used in the path of transmitting, receiving and processing packets.
- Security risk: Vulnerability to attacks represented by average path risk factor R path (Equation 17).
- MAC Overhead: MAC frame encoding / encryption operations time, which is a number of seconds.
- MAC Protection Frequency: Adaptive Security activation rate; Percentage of packets that are being ElGamal encrypted as a result of the risk threshold.
- Computation Time: this is the time spent by the algorithm running, both routing and assessment of fitness and updates.

IX. Results and Analysis

A. *Routing Performance at different attack densities*

TABLE VI shows the comparison between the performance of SI-SLnO and baseline algorithms within four settings of attack density 25, 50, 75, and 100 infected devices on a 250-node network.

Key Observations:

Total Cost Reduction: SI-SLnO with 25 infected devices has minimum cost of 0.56, which is better than GA (13.78%), PSO (10.04%), FF (7.50%), CS (4.69%), LA (0.57%), and CM-LA (6.23%). This illustrates the best multi-objective optimization between the security and performance.

Scalability of Attack Density: Once the infected devices reach 100, SI-SLnO continues to have the lowest cost (0.62), whereas the cost of GA reaches 0.74 (19.35%). This implies strong attack resistance by means of successful exclusion of malicious nodes.

PDR Maintenance: SI-SLnO maintains PDR of over 95% at all attack densities, which is much better than GA (82% with 100 infected devices) and PSO (87%). Attack detection based on rules are effective in detecting and avoiding black hole/selective forwarding nodes.

Energy Efficiency: SI-SLnO is 12-15% less in energy consumption as compared to GA/PSO since the shorter straight routes incur less energy because of the absence of circuitous routes caused by evil nodes.

B. *Convergence Analysis*

There is convergence behavior of SI-SLnO and baseline algorithms as shown in table VII using 50 infected devices and 100 iterations.

Analysis:

- Rapid Early Convergence: SI-SLnO gets almost optimal solutions in the 40 th iteration (cost = 0.592) and GA in 75 iterations (cost = 0.625) to get similar quality solutions.
- Escape local optima: SI-SLnO shows better performance (cost is 12.96% lower than GA, 7.64 lower than PSO) at iteration 60, which can be explained by the self-improvement mechanism compelling exploration as the fitness levels off.
- Finally, Solution Quality: SI-SLnO reaches a final cost of 0.585 averaging over 100 iterations better than CM-LA by 1.85. This confirms increased power of attack by sea lions in a particular phase than in hybrid Cuckoo-Lion method.
- Consistency: The final solutions of SI-SLnO have a standard deviation of 0.0047, which is lower than GA (0.0182) and PSO (0.0135) showing a stable convergence.

i) Granularity of Security Performance.

Table 3 demonstrates the MAC Overhead Analysis:

MAC overhead is measured at different network scales (250-1000 nodes) and risk levels (0.3- 0.7).

• Threshold 0.3: SI-SLnO has MAC overhead of 0.3 seconds with 500 nodes, which is 25 and 20 percent less than GA, CS, CM-LA (0.4 seconds) and PSO, FF, LA (0.375 seconds). Aggressive risk minimizes the encryption activation.

This indicates that SI-SLnO (threshold 0.4) has improved 16.28% compared to GA, 18.6% compared to CS, 23.26% compared to PSO, and 25.58% compared to CM-LA. The best tradeoff between security coverage and computational cost.

• Threshold 0.7 (Conservative): SI-SLnO manages to cut MAC overhead in 750 nodes by 34.62 percent of PSO. High threshold makes maximum use of adaptive security, encrypting only the potentially really dangerous paths.

• Scalability: SI-SLnO MAC overhead increases sub-linearly (37%), whereas GA increases nearly-linearly (92%), with increasing the size of the network (250 nodes to 1000 nodes).

Table VI. Total routing cost comparison across attack densities (lower is better)

Infected Devices	GA	PSO	FF	CS	LA	SI-SLnO
25	0.631	0.616	0.602	0.587	0.563	**0.560**
50	0.682	0.678	0.648	0.620	0.603	**0.585**
75	0.694	0.683	0.661	0.642	0.621	**0.601**
100	0.740	0.728	0.695	0.668	0.641	**0.620**

ii) Cross-Layer Security Performance

MAC Overhead Analysis table VII demonstrates the MAC Overhead Analysis:

MAC overhead is measured at different network scales (250-1000 nodes) and risk levels (0.3- 0.7).

• Threshold 0.3: SI-SLnO has MAC overhead of 0.3 seconds with 500 nodes, which is 25 and 20 percent less than GA, CS, CM-LA (0.4 seconds) and PSO, FF, LA (0.375 seconds). Aggressive risk minimizes the encryption activation.

This indicates that SI-SLnO (threshold 0.4) has improved 16.28% compared to GA, 18.6% compared to CS, 23.26% compared to PSO, and 25.58% compared to CM-LA. The best tradeoff between security coverage and computational cost.

• Threshold 0.7 (Conservative): SI-SLnO manages to cut MAC overhead in 750 nodes by 34.62 percent of PSO. High threshold makes maximum use of adaptive security, encrypting only the potentially really dangerous paths.

• Scalability: SI-SLnO MAC overhead increases sub-linearly (37%), whereas GA increases nearly-linearly (92%), with increasing the size of the network (250 nodes to 1000 nodes).

Table VII. MAC overhead (seconds) across network scales at threshold 0.4

Nodes	Threshold	GA	PSO	FF	CS	LA	SI-SLnO
250	0.4	0.50	0.45	0.45	0.45	0.45	**0.40**
500	0.4	0.70	0.70	0.70	0.70	0.70	**0.52**
750	0.4	0.80	0.80	0.65	0.65	0.65	**0.55**
1000	0.4	0.95	0.95	0.75	0.75	0.75	**0.65**

MAC Protection Frequency:

This measure is a measure of how often adaptive security switches to encryption, and it represents the level of intelligence of the protocol to differentiate between safe and unsafe paths.

Threshold 0.4: SI-SLnO is able to reach 40% MAC protection frequency (250 nodes), which is 20% lower than competing algorithms (50%). This implies better direction to choose without encrypting the high-risk areas hence saving needless overhead of encryption and still maintaining the security.

• Threshold 0.7: The protection frequency is decreased to 30% of SI-SLnO and 50% of baselines (twenty percent better). Low risk path identification is extensively exploited by conservative threshold.

Energy-Security Trade-off: Reduced frequency of protection is directly proportional to savings of energy. SI-SLnO uses about 500 nodes with threshold 0.4 consumes less energy (at 18 percent) than GA because of less cryptographic work but same level of security coverage (both have 0 percent black hole attacks).

iii) *Security Risk Minimization*

Table VIII displays security risk analysis versus node counts versus security thresholds.

Key Findings:

• Risk Reduction: SI-SLnO has a security risk of 0.20658 with 250 nodes, which is significantly less than CM-LA (0.23736), GA (0.23829) and PSO (0.23246). This 13.36 percent increase against GA depicts good malicious node avoidance.

Large-Scale Networks: SI-SLnO exhibits a risk of 0.27, whereas traditional methods and techniques increase to 0.70 (159% more). Efficient FNT filtering and attacks based on PDR are the reason behind scalable risk management.

• Threshold Sensitivity: The higher the threshold, the less risk (0.7 vs. 0.3) in all algorithms, yet 2.5x more sensitive to security policy changes shows better responses to SI-SLnO.

Table VIII. Security risk factor comparison (lower indicates better security)

Nodes	Threshold	GA	PSO	FF	CS	LA	SI-SLnO
250	0.4	0.23829	0.23246	0.23430	0.21744	0.22029	**0.20658**
500	0.4	0.70	0.70	0.70	0.70	0.70	**0.27**
750	0.4	0.68	0.68	0.54	0.54	0.54	**0.32**
1000	0.4	0.75	0.75	0.60	0.60	0.60	**0.38**

iv) Computation Time Overhead

We compares computation time of various protocol elements: optimal route selection, cross-layer security choice, MAC security, and overall overhead.

Results:

Path Selection Time SI-SLnO is 1.8-2.2 seconds to discover a route (250-1000 nodes), or 250-1000 nodes or 15 percent faster than PSO (1.9-2.4s) and 200 times faster than GA (2.1-2.6s). Low overhead is assisted by efficient fitness testing and focused search.

Cross-Layer Security Decision: Risk threshold evaluation costs no more than 0.05-0.08 seconds, which is less than 4 per cent overhead. Simple arithmetic on pre-calculated R f values is guaranteed by lightweight computation to make it real-time applicable.

MAC Protection Time: ElGamal operations increase by 0.3-0.5 seconds per packet in the case of encryption being used. Adaptive security however slows average encryption frequency to 40 percent and achieves effective overhead of 0.12-0.20 seconds, which is lower than always-on encryption schemes (0.3-0.5 seconds).

Total Overhead: The end-to-end protocols (discovery + security decision + MAC) take 2.0-2.5 seconds which falls within acceptable latency ranges of an IoT application (usually less than 5s tolerance). This is between 12-18% less than GA-based approaches.

v) Statistical Validation

Table IX. Statistical analysis of SI-SLnO performance (10 runs, 50 infected devices, threshold 0.4)

Nodes	Metric	Mean	Median	Std Dev	Improvement vs. GA
250	Cost	0.560	0.558	0.0047	8.18%
	PDR (%)	96.2	96.5	1.23	12.5%
	Risk	0.2066	0.2055	0.0089	13.4%
500	Cost	0.585	0.583	0.0052	5.68%
	PDR (%)	95.8	96.0	1.45	10.2%
	Risk	0.2700	0.2680	0.0125	61.1%
1000	Cost	0.620	0.618	0.0063	4.21%
	PDR (%)	94.5	94.8	1.67	8.5%
	Risk	0.3800	0.3750	0.0182	49.3%

Statistical Significance:

Compared to each of the baseline algorithms, paired t-tests of SI-SLnO have statistically significant high ($p < 0.01$) performance in all metrics (cost, PDR, risk) at network sizes of 250 nodes or greater. The size of the effects (Cohen d) is between 1.2 and 2.8 which implies huge real world implications.

X. DISCUSSION

The overall analysis proves the efficiency of SI-SLnO in several aspects:

Optimization Performance:

The self-improvement mechanism can make SI-SLnO achieve better performance in comparison to six state of the art algorithms. The adaptive stage choice using the feedback of fitness helps to avoid premature convergence (as in GA/PSO) and provides efficient exploration (better than pure exploration algorithms such as FF/CS).

Security Efficacy:

Attack detection using rules is able to detect malicious nodes with 98.5 percent accuracy (which was confirmed using controlled experiments where positions of the attackers are known). The cross-layer risk analysis appropriately focuses on the security-critical paths to be encrypted and spares energy on the secure paths.

Scalability:

SI-SLnO exhibits sub-linear deterioration with respect to network size with increasing number of nodes, 250 to 1000 nodes, which is due to efficient FNT filtering that minimizes the search space. MAC overhead only increases 37 percent with 4-fold node increase, confirming the relevance of protocol to massive IoT implementations.

Real-World Applicability:

The calculation time of the protocol (2-2.5 seconds to find a route) is within the range of the IoT update cycle (10-60 seconds to report sensor measurements). Reduction in energy consumption (12-15) is directly proportional to longer device life- which is important in battery-powered sensors in remote systems.

Limitations and Trade-offs:

ElGamal encryption was secure but also gave 0.3-0.5s latency on the packets with the encryption on. In cases where ultra-low-latency is needed (less than 100ms), alternative lightweight ciphers (e.g. AES-128) can be used at slight cost in security.

- Attack detection using PDR needs 50-packet observation window, which will add 10-50s of detecting latency to traffic rate. This can be tolerated by applications that can be attacked in the short term, and critical systems can size windows smaller, at the expense of false positives.

The protocol presupposes the relaxed time synchronization of the timestamps to detect the attacks. Other forms of correlation (e.g. sequence number analysis) might be required in very mobile or asynchronous networks.

A. Conclusions and Future Work

In this paper, an original secured cross-layer protocol, SI-SLnO, was introduced that combines Self-Improved Sea Lion Optimization and adaptive MAC-layer security to IoT networks. The protocol fills important gaps of the current methods with the integration of multi-objective routing optimization, integrated multi-attack detection, and dynamic security policy enforcement on both MAC and routing layers.

The role of simulations Vast simulations on a variety of network structures (250-1000 nodes, 25-100 infected devices, different risk thresholds) have shown:

- Reduction of the routing cost by 13.78 percentage.
- MAC overhead reduction of 25.58% through intelligent encryption enabled only on high-risk paths and saved on computational resources.
- Reduction of security risk to 0.20658 which is significantly lower than the state-of-the-art schemes, and PDR above 95.
- Effective detection and prevention of black hole, selective forwarding, and wormhole attacks by using lightweight PDR-based behavioral analysis.

The framework suggested above is practically viable to implement the IoT resources-constrained deployments in the smart cities (environmental monitoring, traffic management), industrial automation (equipment health monitoring) and in healthcare (patient vital signs tracking) where security and energy efficiency are the main concerns.

B. Future Research Directions

There are a number of potential avenues that should be researched:

1. Machine Learning Integration: Adding lightweight machine learning models (e.g. decision trees, SVM) to rule-based attack detection would help increase the accuracy of unknown attack patterns at a reasonable computational cost on IoT devices.

2. Multi-Objective Optimization Revision: Adding other goals like network lifetime balance (the equalisation of energy consumption among the nodes) and QoS differentiation (priority routing of important data) would provide more dimensions in protocols.

3. Mobility Support: SI-SLnO needs to be extended to mobile IoT networks (vehicular networks, wearable devices) and therefore dynamic path re-optimization and handoff mechanisms are needed. Pro-active re-routing may be caused by predictive mobility models prior to the occurrence of link failures.

4. Quantum-Resistant Cryptography: Since the development of quantum computing will compromise the existing cryptosystems of generating a public-key, the introduction of post-quantum resistant cryptosystems (e.g., lattice-based encryption) to the security stack of MAC-layer will guarantee future-resistance.

5. Federated Security Intelligence: Multiple gateways in the IoT can achieve better detection of attacks and could also collaboratively respond to threats without the overhead of a central point of coordination.

6. Hardware Acceleration: ElGamal encryption or SI-SLnO fitness evaluation implementations using FPGA or ASIC and potentially 10-100x faster than an ARM would be of interest because with under one second to compute a route, then time-constrained applications can be run.

7. Energy Harvesting Integration: The integration of risk thresholds and encryption policy can be adjusted depending on the rate of energy harvesting (solar, RF, vibration), which would allow self-sustainable secure execution of sensor networks in an always-on network.

C. Concluding Remarks

The merging of the IoT spread, advanced cyber threats, and limited resources are creating the need to develop novel cross-layer security paradigms. SI-SLnO shows that bio-inspired optimization together with intelligent security adaptation can all be used to achieve performance, security, and energy efficiency, three goals, which usually conflict. The protocol can offer the basis of next-generation secure IoT architectures by connecting MAC and routing layers with risk-aware intelligence in a way that it can function reliably in adversarial and resource-limited operational conditions.

Likely, protocols such as SI-SLnO, which trade rigor of security with the performance of a system in safety-critical systems (autonomous vehicles, medical implants, critical infrastructure), will be critical facilitators towards reliable ubiquitous computing as IoT ecosystems continue to diversify into safety-critical systems.

XI. REFERENCES

[1] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[2] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

[3] Gartner Inc. (2017). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Retrieved from https://www.gartner.com/newsroom/id/3598917

[4] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28. https://doi.org/10.1016/j.jnca.2017.04.002

[5] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142. https://doi.org/10.1109/JIOT.2017.2683200

[6] Zhang, Y., & Li, P. (2015). Physical-layer security for IoT: A comprehensive survey. IEEE Communications Surveys & Tutorials, 17(3), 1620-1645.

[7] IEEE Standard 802.15.4-2015. (2016). IEEE Standard for Low-Rate Wireless Networks. IEEE Computer Society. https://doi.org/10.1109/IEEESTD.2016.7460875

[8] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J., & Alexander,

R. (2012). RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550. https://doi.org/10.17487/RFC6550

[9] Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). FairAccess: A new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks, 9(18), 5943-5964. https://doi.org/10.1002/sec.1748

[10] Rault, T., Bouabdallah, A., & Challal, Y. (2014). Energy efficiency in wireless sensor networks: A top-down survey. Computer Networks, 67, 104-122. https://doi.org/10.1016/j.comnet.2014.03.027

[11] Kawamoto, Y., Nishiyama, H., Kato, N., Yoshimura, N., & Yamamoto, S. (2016). A traffic distribution technique to minimize packet delivery delay in multilayered satellite networks. IEEE Transactions on Vehicular Technology, 65(4), 2315-2324.

[12] [12] Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561. https://doi.org/10.17487/RFC3561

[13] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646. https://doi.org/10.1109/JIOT.2016.2579198

[14] Chen, M., Miao, Y., Hao, Y., & Hwang, K. (2017). Narrow band Internet of Things. IEEE Access, 5, 20557-20577. https://doi.org/10.1109/ACCESS.2017.2751586

[15] Dvir, A., Holczer, T., & Buttyan, L. (2011). VeRA - Version Number and Rank Authentication in RPL. Proceedings of IEEE MASS 2011, 709-714. https://doi.org/10.1109/MASS.2011.76

[16] Sastry, N., & Wagner, D. (2004). Security considerations for IEEE 802.15.4 networks. Proceedings of ACM WiSe 2004, 32-42. https://doi.org/10.1145/1023646.1023654

[17] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.

[18] Abid, K., & Pathak, N. K. (2024). Blockchain-Enhanced Authentication for Wi-Fi Probe Networks: Evaluating Performance Against Security Attacks. Journal for Basic Sciences, 24(9), 207-217. ISSN 1006-8341.

[19] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646.

[20] Rault, T., Bouabdallah, A., & Challal, Y. (2014). Energy efficiency in wireless sensor networks: A top-down survey. Computer Networks, 67, 104-122.

[21] Li, W., Tug, S., Meng, W., & Wang, Y. (2020). Designing collaborative blockchained signature-based intrusion detection in IoT environments. Future Generation Computer Systems, 96, 481-489. https://doi.org/10.1016/j.future.2019.02.064

[22] Holland, J. H. (1992). Genetic Algorithms. Scientific American, 267(1), 66-73.

[23] Kennedy, J., & Eberhart, R. (1995). Particle swarm optimization. Proceedings of IEEE ICNN, 4, 1942-1948. https://doi.org/10.1109/ICNN.1995.488968

[24] Yang, X.-S. (2009). Firefly algorithms for multimodal optimization. Stochastic Algorithms: Foundations and Applications, 169-178. https://doi.org/10.1007/978-3-642-04944-6_14

[25] Yang, X.-S., & Deb, S. (2009). Cuckoo search via Lévy flights. Proceedings of World Congress on Nature & Biologically Inspired Computing, 210-214. https://doi.org/10.1109/NABIC.2009.5393690

[26] Abid, K., & Pathak, N. K. (2024). Adaptive Random MAC Strategy for IoT Security Through Network Forensics Investigation. J. Electrical Systems, 20(7s), 1740-1748.

[27] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of ACM MobiCom, 255-265. https://doi.org/10.1145/345910.345955

[28] Buchegger, S., & Le Boudec, J.-Y. (2002). Performance analysis of the CONFIDANT protocol. Proceedings of ACM MobiHoc, 226-236. https://doi.org/10.1145/513800.513828

[29] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1(2-3), 293-315. https://doi.org/10.1016/S1570-8705(03)00008-8

[30] Hu, Y.-C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks in wireless networks. Proceedings of IEEE INFOCOM, 1976-1986. https://doi.org/10.1109/INFCOM.2003.1209219

[31] Lazos, L., Poovendran, R., Meadows, C., Syverson, P., & Chang, L. W. (2005). Preventing wormhole attacks on wireless ad hoc networks: A graph theoretic approach. Proceedings of IEEE WCNC, 2, 1193-1199.

[32] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 12-22. https://doi.org/10.1109/MPRV.2018.03367731

[33] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768. https://doi.org/10.1016/j.future.2017.08.043

[34] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018

[35] Kamgueu, P. O., Nataf, E., & Ndié, T. D. (2018). Survey on RPL enhancements: A focus on topology, security and mobility. Computer Communications, 120, 10-21. https://doi.org/10.1016/j.comcom.2018.02.011

[36] Ben-Othman, J., & Yahya, B. (2010). Energy efficient and QoS based routing protocol for wireless sensor networks. Journal of Parallel and Distributed Computing, 70(8), 849-857.

[37] Kim, D., Garcia-Luna-Aceves, J. J., Obraczka, K., Cano, J.-C., & Manzoni, P. (2003). Routing mechanisms for mobile ad hoc networks based on the energy drain rate. IEEE Transactions on Mobile Computing, 2(2), 161-173.

[38] Masadeh, R., Mahafzah, B. A., & Sharieh, A. (2019). Sea Lion Optimization Algorithm. International Journal of Advanced Computer Science and Applications, 10(5), 388-395. https://doi.org/10.14569/IJACSA.2019.0100548

[39] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4), 469-472. https://doi.org/10.1109/TIT.1985.1057074I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[40] K. Elissa, “Title of paper if known,” unpublished.

[41] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[42] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[43] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[44] Electronic Publication: Digital Object Identifiers (DOIs):

[45] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467. **(Article in a journal)**

[46] H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670. **(Article in a conference proceedings)**