Iraqi Journal of Information and Communications Technology(IJICT)
Vol. 9, Issue 1, April 2026
www.ijict.edu.iq
ISSN:2222-758X
e-ISSN:2789-7362

IAE-CRP IMPROVED ANT OPTIMISATION WITH ECC-BASED CLUSTERED ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORK

Sami Abduljabbar Rashid[1], Humam Hussein[2,3], Taha A. Elwi[4], Mohammed Salah Abood[5], Mustafa Maad Hamdi[6]

[1] Biomedical Engineering Research Centre, University of Anbar, Ramadi, Anbar, Iraq
[2] College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq
[3] Avicenna E-Learning Center, Tikrit University, Tikrit, Iraq
[4] Department of Automation and Artificial Intelligence Engineering, College of Information Engineering, Al-Nahrain University, Jadriya, Baghdad, Iraq
[5] Faculty of Information and Electronics Engineering, Beijing Institute of Technology, Beijing, China
[6] Department of Computer Science, College of Computer Science and Information Technology, University of Anbar, Ramadi, Anbar, Iraq
sami.abduljabbar.rashid@uoanbar.edu.iq[1], humam.n.hussein@tu.edu.iq[2,3], taelwi82@gmail.com[4], mohammedsalah@bit.edu.cn[5], Mustafa.maad.hamdi@uoanbar.edu.iq[6]
Corresponding Author: **Taha A. Elwi**
Received:22/09/2025; Revised:22/12/2025; Accepted:27/04/2026
DOI:10.31987/ijict.9.1.353

***Abstract*- The speedy improvement in Wireless Sensor Network (WSN) technology leads to various applications such as smart cities, industrial applications, and health care. Energy efficiency is one of the leading challenges in WSN because the major constraints for the process of communication are the routing protocol and energy efficiency. A new approach has been introduced to enhance network performance and quality, an improved Ant Colony Optimisation (ACO) with Elliptic Curve Cryptography (ECC) mechanism-based Clustered Routing Protocol for WSN. The major sections of the protocol are LEACH-based CH selection, Ant Colony Optimisation, and ECC mechanism. The protocol offers improved results in optimal path finding and wormhole attack protection. Simulation results indicate that the proposed scheme yields superior performance metrics in terms of Packet Delivery Ratio (PDR), network throughput, energy consumption, and security overhead.**

keywords: **Wireless Sensor Networks (WSN), Energy Efficiency, Cluster-Based Routing, Ant Colony Optimisation (ACO), Elliptic Curve Cryptography (ECC), Wormhole Attack Detection, Secure Communication, Network Lifetime, Packet Delivery Ratio (PDR), Network Throughput.**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have extended their scope of research and have been implemented in various sectors, such as agriculture, smart home automation, health monitoring, industrial oversight, and environmental control [1]. The sensor first detects changes in its surrounding physical environment, then it processes the readings and finally sends the data to the Base Station (BS) via the routing protocol. This data communication is what uses a lot of the energy, which in return causes the performance and lifetime of WSNs to be adversely affected [2]. Sensors that are battery-powered usually have a short life due to the limited battery capacity. In a star topology network, energy distribution among nodes becomes a problem. Although a variety of solutions have been put forward to overcome this constraint, it is still an area of concern that is being explored continually [3]. The efficiency and duration of the network depend on the amount of

energy that nodes have. Energy is consumed in different ways, such as changing modes from active to sleep and vice versa, data transmission, routing overhead, and handling network collisions [4][5]. One of the major challenges in WSNs is the trade-off between energy conservation and the provision of secure transmission of confidential data [6-9]. This study is mainly concerned with the following important contributions:

- Innovative Hybrid Routing Protocol: The IAE-CRP protocol that fuses LEACH-based cluster-head selection with ACO and ECC, thus attaining a balanced improvement in both energy efficiency and network security for wireless sensor networks.
- Integrated Wormhole-Attack Defence: Added a secured-in mechanism that can detect and neutralise wormhole attacks, thus the reliability and confidentiality of data transmission in adversarial environments have been strengthened.
- Comprehensive Performance Gains: The newly designed protocol outperformed the existing (SEEPOT and SLTBT) methods in NS2 simulations, as evidenced by the considerable improvements in packet delivery ratio, network throughput, energy consumption, and packet loss, thus enabling a longer network lifetime and higher operational efficiency. Energy-efficient and secure routing are crucial in WSNs for IoT, smart cities, industrial monitoring, and healthcare due to persistent energy and security challenges. The IAE-CRP protocol delivers impressive results with a 96.87% PDR, 534.87 kbps throughput, energy consumption of 0.15J, security overhead of 8.0 ms per packet and includes wormhole protection through algorithms such as LEACH, ACO, and ECC.

This paper is divided into different sections: Section II examines the research done on the energy-efficient and routing methods in wireless sensor networks. Section III explains the proposed IAE-CRP protocol that includes the radio-energy consumption model, cluster-head selection based on LEACH, and the improved Ant Colony Optimisation operation. Section IV is about the wormhole attack threat model and its defence mechanism. Section V elaborates on the method of creating the key utilising ECC and the secure communication process. Section VI is about performance evaluation, simulation setup, and comparative analysis with existing protocols. In Section VII, ends with suggestions for future research.

II. LITERATURE REVIEW

This section analyses various path optimisation strategies, referencing the work of Aparna Ashok Kamble and B.M. Patil [10], multiple optimisation techniques and evaluates the pros and cons of traditional path optimisation models. Walid Osamy and Ahmed A. El-Sawy [11], an optimisation strategy for WSN focused on reducing energy consumption. It employs a clustering method based on competitive swarm optimisation supported by genetic algorithms. To enhance network performance related to energy consumption, Etobi Damian, Williams-Paul, et.al [12], developed three approaches: the PRI method, the NSI algorithm, and a proactive feedback technique.

Daneshvar, Pardis Alikhah, et. al [13], a routing model for WSN that utilises the GWO for selecting CH. However, the energy efficiency benefits may not be observed in networks with a large number of sensors. Vinitha, Rukmini, et al. [14] introduced a Taylor C-SSA model designed for energy-efficient multi-hop routing in WSNs. Yet, the evaluation of the model's performance across relevant experimental metrics remained insufficient. Amir Seyyed Abbasi and Farzad Kiani [15] designed a routing model based on improved ACO for providing an optimal path for data transmission. This system is

ISSN:2222-758X
e-ISSN:2789-7362

effective in terms of energy consumption. Mohammed Farsi, Mahmoud Badawy, et.al [16] developed a congestion-aware clustering with Primary Cluster Head (PCH) and Secondary Cluster Head (SCH) selection.

Kalaivanan and Bhanumathi [17] introduced the CTEEDG protocol employs Fuzzy logic to select the CH. Simulation results demonstrate that this approach enhances throughput and energy efficiency. Hassan, Abdellah Najid [18] developed an enhanced clustering hierarchy algorithm to achieve higher energy efficiency in a wireless sensor network by using a sleeping and waking mechanism. Alessandro Di Stefano, Aurelio La Corte, et.al [19] created a multi-agent model that utilises a hierarchical clustering method along with an aggregation and rejection mechanism. Zhidong Zhao, Duoshui Shi, et.al [20] used traditional hierarchical clustering to manage total energy consumption. A dynamic method that includes a dual CH quarters strategy and an optimal CH function.K. Thangaramya, K. Kulothungan, et.al [21] designed a Neuro-Fuzzy Rule-Based Cluster Formation aimed at improving the QoS in network systems.

Ramya Kulandaivel, S. Periyanayagi, et al. [22] introduced two sets of nodes: sensors and actors, to sense the surrounding environment. Ming Tao, Xueqiang Li, et.al [23] analysed the deployment and connectivity issues in a network. It proposes a multi-objective joint optimisation model incorporating multiple constraints to resolve these issues. Sachin Sen and Chandimal Jayawardena [24] developed a new energy balancing technique to improve reliability and cybersecurity. Divya R., Dr R.Chinnaiyan [25] developed a model to improve the security so as to protect the network from the DOS attacks. N. Prakash. Dr M. Rajalakshmi, et.al [26], the model created focuses on improving energy efficiency and network security. The authors emphasise optimising performance in next-generation communication and computing paradigms by using intelligent, decentralised, and predictive methodologies to tackle emerging issues like end-to-end delays [27], Blockchain/distributed ledger [28][29], Routing improvements [30], Machine learning (LSTM, ML models) [31][32].

III. PROPOSED MODEL

The hybrid protocol design uses LEACH-based clustering for cluster head selection, ACO for dynamic routing paths, and ECC/ECDH for secure key generation. It addresses energy constraints, optimal routing, and security concerns like wormhole attacks in WSNs. Fig. 1 explains the proposed flowchart in detail.

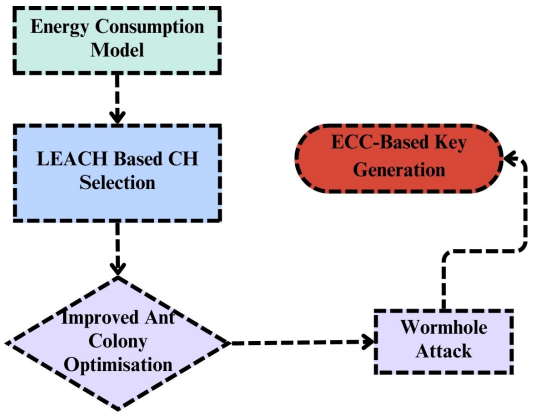

Figure 1: Proposed model flowchart.

ISSN:2222-758X
e-ISSN:2789-7362

A. Energy Consumption Model

Under the constructed wireless sensor networks, the radio energy conservation model is analysed, where m represents the bit message for the distance d [5]. Hence, the transmission is given in Eq. (1) as follows.

$$E_{tx}(m,d) = \begin{cases} mE_{elec} + m\epsilon_{fs}d^2, & d < d_0 \\ mE_{elec} + m\epsilon_{mp}d^4, & d \geq d_0 \end{cases} \tag{1}$$

Eq. (1) represents the transmission energy consumption for sending an m-bit packet over distance d. When the transmission distance is less than the threshold distance d_0, the free-space propagation model is used with energy factor ε_{fs}. Otherwise, the multipath fading model is adopted with energy factor ε_{mp}. The same process is applied for calculating the energy dissipated on the receiver side [4], also in Eq. (2).

$$E_{Rx}(m) = m * E_{\text{elec}} \tag{2}$$

Eq. (2) gives the energy dissipated at the receiver side for receiving an m-bit message, where E_{elec} denotes the electronic energy consumed per bit. But for all the calculations, we consider only the communication energy. Eq. (3) gives the energy consumed [6].

$$E_{\text{total}}(m,d) = E_{\text{tx}}(m,d) + E_{\text{rx}}(m) \tag{3}$$

The above Eq. (1) and Eq. (2), the notation E_{elec} indicates the overall energy consumed to transfer or receive an I-bit message. Hence, Eq. (3) represents the total communication energy consumption, which is obtained by summing the transmission energy and the reception energy.

B. LEACH Based CH Selection

The LEACH protocol is designed for sparse sensor networks, primarily focusing on efficiently transmitting data to a sink node. It selects CHs based on energy levels and utilises randomised rotations among them to optimise energy distribution among nodes. The decentralised method removes the requirement for centralised control and global network knowledge, thus intending to increase the network lifespan while not relying on location data. Furthermore, LEACH supports data aggregation at CHs, which is instrumental in reducing network traffic. Overall, it exemplifies a MAC model that ensures efficient data collection and transmission while addressing energy consumption concerns.

The LEACH protocol is applied in rounds after determining the ideal percentage of cluster heads. For each round, a certain number of cluster heads is assigned, based on the total number of rounds. h and the identified cluster heads g. Each round consists of a steady-state phase and a setup phase, the latter being further divided into three sub-phases: advertisement, cluster setup, and broadcast scheduling. During the advertisement phase, each node generates an integer between 0 and 1 and compares it with a predefined threshold level to determine if it becomes a cluster head.

$$T(n) = \begin{cases} \frac{p}{1-p\left(r \bmod \left(\frac{1}{p}\right)\right)}, & \text{if } n \in G \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

ISSN:2222-758X
e-ISSN:2789-7362

Eq. (4) defines the LEACH threshold used for cluster-head selection [8], where p is the desired percentage of cluster heads, r is the current round, and G is the set of nodes that have not served as cluster heads in the last $1/p$ rounds. When a node opts to become a cluster head, it disseminates an announcement packet to its neighbouring nodes, which respond to indicate their participation during the cluster head setup phase. Responses are aggregated during the broadcast phase to establish cluster memberships. The cluster head subsequently generates a TDMA schedule based on all cluster nodes, dictating message transmission intervals. To ensure efficient data transfer, data is initially stored in the cluster head before being relayed to the sink and ultimately to the base station, adhering to the structure outlined in the LEACH protocol.

$$N_{\text{CH}} = p \times N \tag{5}$$

Eq. (5) represents the expected number of cluster heads in the network [6], where N is the total number of sensor nodes and p is the predefined cluster-head probability.

C. Improved Ant Colony Optimisation

Ant colonies are metaheuristic and probabilistic optimisation techniques. It is a bio-inspired algorithm, not followed by a central problem-solving method based on the actual structure and mobility operations of an ant colony. A meta-heuristic algorithm implies that, with minimal modifications to any problem, a particular user optimisation technique or solution may be obtained. In a simple example, two numbers may be added. The additional operation is an algorithm that remains the same, but it may alter the numbers or operands. The ACO utilises a huge number of sophisticated iteration algorithms to solve the issue with the natural behaviour of real-time ants. Ants usually move with the greatest concentration of pheromones, as these are the hormones that guide their behaviour. Other ants may be attracted to the same colony, an ally colony, or even a foe colony. The ants in the system or colony migrate from one x node to another y node at random.

$$P_{xy} = \frac{\tau_{xy}^{\alpha} \eta_{xy}^{\beta}}{\sum \left(\tau_{xk}^{\alpha} \eta_{xk}^{\beta} \right)} \tag{6}$$

Eq. (6) defines the probability of selecting node y as the next hop from node x [9], where $\tau_{x,y}$ denotes the pheromone intensity on edge (x, y), η_{xy} represents the heuristic desirability of that edge, and α and β control the relative influence of pheromone and heuristic information. Thus, after each iteration, pheromone trails may be updated when the ants have completed a correct solution or a tour around the formula.

$$\tau_{xy}(t+1) = (1-\rho)\,\tau_{xy}(t) + \Delta\tau_{xy} \tag{7}$$

Eq. (7) updates the pheromone trail after each iteration [10], where ρ is the evaporation coefficient and $\Delta\tau_{xy}$ is the amount of pheromone deposited on edge (x, y). This indicates that at least some portion of each pheromonal trail may be removed following any iteration, and each iteration will repeat itself. Therefore, when using ACO the overall routing decision for the entire system has a better chance of being accurate because the search for the optimum path has been limited to the immediate vicinity around where ant activity was observed. Each artificial ant travelling from one node to another is therefore subject to the proportionality principle; the probability that ant k will travel from node x to y is proportional to a randomly selected z distributed uniformly within the interval [0,1].The intrinsic parallel nature of ACO makes it an

ISSN:2222-758X
e-ISSN:2789-7362

excellent candidate for fast response to feedback and therefore selection of optimum routes, not only within WSNs but also for many other applications. As a result of the final process of vapourisation , all pheromone quantities are then re-evaluated through the comparison of the original pheromonal quantities against the newly-created quantities. Therefore, as ants progress along a given path, they change all of the previously established quantities of the respective pheromonal trails. In order to prevent an undesirable and often dangerous state from occurring, it is important to monitor the update process. This state can occur when the update stops for some reason and the ants then proceed to build the same solutions over and over, without ever bothering to seek alternative paths to reach their destination.

Thus, for node routing problems, the ACO algorithm can be applied in order to identify optimal solutions to minimize the total amount of latency experienced by a network system as well as to address other limitations encountered that prevent WSN systems from gaining the advantage of this methodology. The excess of available protocols for various types of mode networks has made it difficult to determine which protocol should be used in a particular situation. Previous methods had primarily focused on increasing a system's performance or reducing energy consumption. Common drawbacks of these methods included excessive latency or an inability for data to reach its destination due to the WSN system's high degree of mobility. This research proposes a biologically inspired ACO methodology that employs the use of artificial ants and artificial neighbours. Pheromones should be evaporated or redeposited in priority order so they do not have an impact on the system with a circular loop dependency (no repeating path). This allows for improved searching for new routes in the ACO algorithm. An upgrade to the enhanced ACO algorithm includes integrating LEACH-based cluster head selection and advanced pheromone management methods. This enhancement helps address issues like path stagnation and circular loops common in basic ACO strategies. In traditional ACO, ants can get stuck on heavily pheromone-laden but inefficient routes in dynamic WSNs, causing higher latency and energy consumption. The improved algorithm tackles these problems by using controlled evaporation and creating artificial neighbours for diverse route exploration. Two evil nodes (M1, M2) in the network conduct a wormhole attack by creating fake short routes. Important considerations include node locations being unknown, cryptographic keys cannot be breached, transmission range less than or equal to d_{max}, and loose synchronisation with RTT. Detection methods focus on identifying disparities in hop-count, RTT, and neighbour overlap by comparing the advertised topology with the actual network structure.

IV. WORMHOLE ATTACK

In a wormhole attack, an attacker intercepts packets at one location while tunnelling them to another, resulting in network oscillation. If the tunnelling exceeds the single-hop transmission range, the attacker can enhance the transmission metrics significantly. By utilising a single-hop radial wireless mode, data can be transmitted immediately via the wormhole, reducing latency. The attacker may initiate the operation before portions of packets are targeted, allowing them to eavesdrop and tunnel the data to an accomplice. Surprisingly, if conducted transparently and dependably, the tunnelling by the attacker may provide efficiency benefits by effectively connecting the network.

In a wormhole attack, the attackers build up solid connections with other nodes in order to have optimal placement for an attack. Even when there is a high degree of authentication and no cryptographic key material, vulnerabilities still exist. The attackers will work together at both ends of the wormhole, and there may not be an obvious difference between the

ISSN:2222-758X
e-ISSN:2789-7362

two nodes involved. However, because the nodes will see packet broadcasts, most ad hoc routing protocols are particularly susceptible to this type of attack.

Wormholes pose a threat to on-demand relaying protocols such as Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). An attack is achieved when an attacker tunnels ROU_REQ packets directly to the final destination. A neighbouring node that receives this packet will therefore retransmit it using the normal routing protocol and will not retransmit ROU_REQ packets that are already in the current setup phase. As a result, it can effectively hide routes that are beyond the wormhole and possibly restrict the area of search to only a few hops if the attacker is close to the originator of the route.

V. ECC-BASED KEY GENERATION

To secure efficient communication in WSNs. It emphasises the importance of utilising encryption keys for both encryption and decryption alongside authentication measures to secure communication pathways. To strengthen network security, the process can be divided into two phases: enrollment and communication.

A. Enrollment Phase

During this enrollment phase, every time a node joins the admissions process, it must be enrolled by the certifying authority (CH). Therefore, we assume that the CH functions as a certifying authority for node enrollment. The enrolment phase also establishes a method to create the public key encryption system used throughout the Assignment. The certifying authority gives the network permission to send private and public keys via a secure way of transferring data.

Our system, based on the ECC system, will require that the Certificate Authority (CA) to create secure keys for the sensors. The ECC algorithm generates a key size of 160 bits which is considered to be much more secure than traditional asymmetric RSA (which has a key size of 1024). The Security of the ECC system is based on the use of the Elliptic Curve Discrete Logarithm Problem (ECDLP). The ECC system uses asymmetric cryptographic technology in the creation and exchange of priv/pub keys. The private key is only used by the owner of that key and its related public key will be distributed to others who may be involved in a transaction that utilizes the public key. A formal and complete mathematical description of the ECC system and its components will be provided [13].

$$y^2 = x^3 + ax + b \tag{8}$$

Eq. (8) gives the general Weierstrass form of an elliptic curve used in ECC, where a and b are curve parameters [13].

$$4a^3 + 27b^2 \neq 0 \tag{9}$$

Eq. (9) ensures that the elliptic curve is non-singular and therefore valid for cryptographic operations [14]. Different curves are used for different values of (a, b) in the case of elliptic curves. The public key is found by the private key "e" multiplied by a Generator point (G) of the particular curve, the consequent point on the curve being the public key (P).

$$Q = dG \tag{10}$$

ISSN:2222-758X
e-ISSN:2789-7362

Eq. (10) represents the ECC public key generation process [3], where d is the private key and G is the generator point on the elliptic curve. ECC operates on elliptic binary curves over a field GF(2m) defined by two parameters a and b (where $b0$ id belongs to GF(2m). It includes an infinite point O and all points (x, y) satisfying the specified equation (11).

$$E(F_p) = \{(x, y) \in F_p : y^2 \mod p = (x^3 + ax + b) \mod p\} \cup \{O\} \tag{11}$$

Eq. (11) defines the elliptic curve over the finite field F_p, including all points that satisfy the curve equation together with the point at infinity [17].

The system by which a vehicle gets its public and private keys from the Certifying Authority is made up of four different stages.

1) A figure "R1" sends a demand for a private key to the Certifying authority by a node encrypting and dispatching the message REQ_MESSAGE. The message encrypted with the public key of the authority contains the ID of R1, the ID of another entity "C," region variables for an Elliptic Curve and a timestamp in Eq. (12) [15].

$$E_{kCA}\left[ID_C \parallel ID_{R1} \parallel (P, a, b, G, n, h) \parallel R_1\right] \tag{12}$$

2) The CA sends the encrypted private key (PRC) to the node that is labelled 'R1.' It also makes sure that the key is provided with the proper identification in Eq. (13) [16].

$$E_{kCA}\left[ID_C \parallel d_C\right] \tag{13}$$

3) Node "R1" sends a REQ_MESSAGE to the certifying authority for the generator (GEN), "C" identification, and a time stamp that has been encrypted with "C's" private key are part of the message in Eq. (14) [17].

$$E_{dA}\left[ID_C \parallel R_2\right] \tag{14}$$

4) The CA will send the GEN to node "R1," along with C's ID and a C-signed time-stamped message encrypted with C's private key in Eq. (15) [18].

$$E_{dA}\left[ID_C \parallel R_2 \parallel G\right] \tag{15}$$

5) Node "R1" is equipped with a private key (dA) and a GEN, so it can generate its own public key (QA) in Eq. (16) [19].

$$Q_A = d_A G \tag{16}$$

Eq. (16) shows how node R1 generates its public key Q_A using its private key d_A and the generator point G.

B. Communication Phase

R1" and "R2" are two nodes that both wish to establish a connection in this phase, and both nodes want to make sure that their messages are legitimate and secure. The research employs the Elliptic Curve Diffie-Hellman (ECDH) method to guarantee secure communication between nodes. ECDH allows the nodes to jointly generate a shared secret key that

ISSN:2222-758X
e-ISSN:2789-7362

will be used for private encryption, thus enabling them to securely exchange messages. The shared key can only be the one derived by nodes that know their individual secret information, thus no other vehicles can eavesdrop on the secure communication, even if there exist adversarial situations. To create a shared secret key, two nodes, "R1" and "R2", have to decide on the Elliptic Curve Domain Parameters. Each node also has a set of public and private keys of its own. Let's suppose that node "R1" has a key pair (dA, QA), where dA is the private key, and QA is the public key. Similarly, node "R2" has a key pair (d_B, Q_B), with dB being the private key and Q_B being the public key. The procedures involved in creating a secret shared key are as follows:

1) Node "R2" sends its public key QB to node "R1", then node "R1" calculates in Eq. (17) [6]:

$$K = d_A \times Q_B \tag{17}$$

Eq. (17) represents the computation of the shared secret key at node R1, where the private key d_A is multiplied by the public key Q_B of node R2. This operation generates a common elliptic curve point that serves as the basis for secure communication.

2) Node "R1" sends its public key QA to node "R2", then node "R2" calculates in Eq. (18) [7]:

$$K = d_B \times Q_A \tag{18}$$

Eq. (18) describes the computation of the shared secret key at node R2, where the private key dB is multiplied by the public key QA of node R1. This ensures that both nodes independently derive the same shared secret.

3) As we all know in Eq. (19),

$$d_A \times Q_B = d_B \times Q_A \tag{19}$$

Eq. (19) demonstrates the fundamental property of the Elliptic Curve Diffie-Hellman (ECDH) protocol, showing that both nodes compute an identical shared secret key despite using different inputs [9]. This equality ensures secure key agreement without directly transmitting the private keys. Since:

$$K = d_A d_B G \tag{20}$$

Eq. (20) expresses the shared secret key generated through ECDH, showing that both communicating nodes derive the same secret point on the elliptic curve [12].

4) So x_k is the shared secret key between two nodes.

VI. PERFORMANCE ANALYSIS

The research utilises Network Simulator 2 (NS2), combining Object Tool Command Language (OTCL) and C++, to simulate the proposed approach in a defined coverage area of 1000 x 1000 meters. A scenario with 100 nodes is executed, incorporating 5% of those as attackers. Key evaluation metrics for comparison include throughput and PDR. To verify

this proposed IAE-CRP is very effective, it is compared with the earlier research, such as SEEPOT and SLTBT. Table I describes the parameters in details.

TABLE I
Simulation Setup and Parameters

Parameter	Value
Simulator	NS2 (OTCL + C++)
Area	1000 × 1000 m
Nodes	100 (+5 attackers)
Traffic Model	CBR/UDP
Packet Size	512 bytes
Packet Rate	4 pkt/s
Sources	20 random to 1 sink
Simulation Time	300 s

A. Network Throughput Calculation

It refers to the rate at which data flows through the network communication channel. The mathematical expression for the calculation of Eq.(21) of throughput is given below [21].

$$\text{Throughput} = \frac{\text{Total received bits}}{\text{Simulation time}} \tag{21}$$

Fig. 2 presents the throughput results of the proposed method alongside its comparison to previous methods. At 100 nodes, IAE-CRP achieves a throughput of 534.87 Kbps, surpassing SEEPOT by 242.1Kbps and SLTBT by 119.5 Kbps. Even at 10 nodes, it delivers 45 Kbps, exceeding SEEPOT by 80 Kbps and SLTBT by 28.6 Kbps. With 40 nodes, the bandwidth hits 180 Kbps, doubling SEEPOT by 112 Kbps and outperforming SLTBT by 64 Kbps. The 100-node test showcases IAE-CRP's scalability, as its throughput is more than three times that of SEEPOT and over double that of SLTBTs.

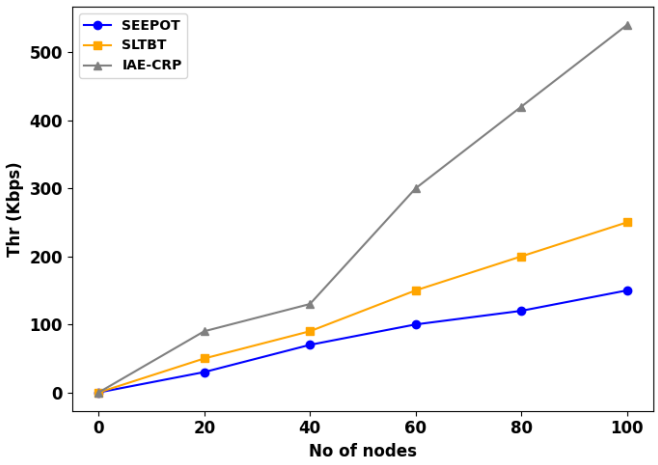

Figure 2: Network throughput calculation

ISSN:2222-758X
e-ISSN:2789-7362

B. Network Packet Delivery Ratio (PDR) Calculation

PDR quantifies the successful transmission of data packets from the source to the destination within a network. A mathematical model is provided in Eq. (22) as in [22].

$$\text{PDR} = \frac{\text{no of packet received}}{\text{Total number of packets sent}} \times 100 \tag{22}$$

Fig. 3 depicts the PDR calculated for the proposed method and earlier methods. At 100 nodes, IAE-CRP obtains the highest Packet Delivery Ratio (PDR) of 96.87%, which represents great leaps of 17.33% and 9.22% over SEEPOT (82.54%) and SLTBT (87.65%), respectively. The figure of 68% marks its PDR at 10 nodes, and it thereby edges out SEEPOT and SLTBT. At 40 nodes, the PDR is 84%, and at 60 nodes, it is 89%.

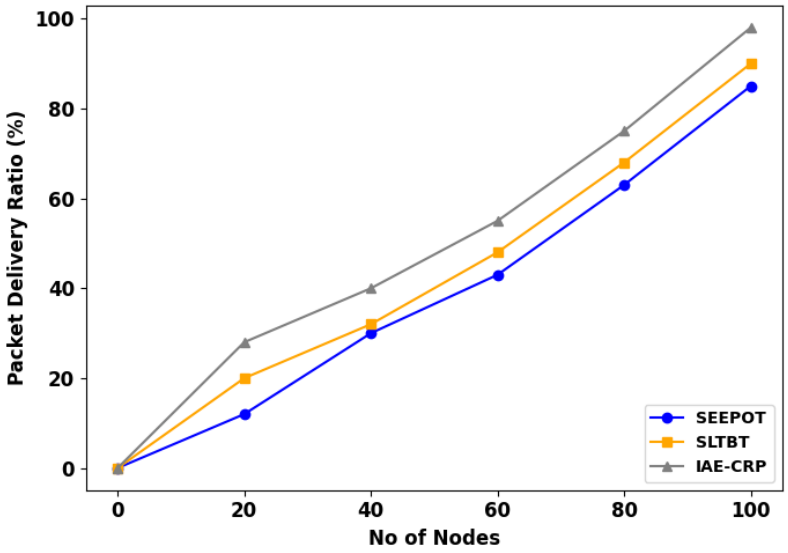

Figure 3: Packet Delivery Ratio (PDR) calculation of the network

C. Energy Consumption

In Fig. 4, the IAE-CRP protocol saves 42-47% energy vs. baseline protocols with 50-100 nodes. Energy use in 50-node scenarios: IAE-CRP is 0.15J, SEEPOT 0.35J, SLTBT 0.28J. At 75 nodes, SEEPOT and SLTBT energy use rise to about 0.42J and 0.35J, while IAE-CRP increases to 0.22J. At 100 nodes, IAE-CRP is 0.28J, less than SEEPOT (0.48J) and SLTBT (0.42J). The IAE-CRP protocol boosts energy efficiency, saving 0.13J on average.

D. Security overhead communication

In Fig. 5, IAE-CRP reduces ECC computation costs by 33%, achieving 8.0 ms per packet, faster than SEEPOT (12.0 ms) and SLTBT (10.0 ms). These results of security against wormhole attacks using a 160-bit ECC based on clustering. Computational time is 8.0 ms, and energy consumption at 100 nodes is only 0.28ms, compared to SEEPOT's 0.48 ms. Table II summarise the comparative analysis of the results.

ISSN:2222-758X
e-ISSN:2789-7362

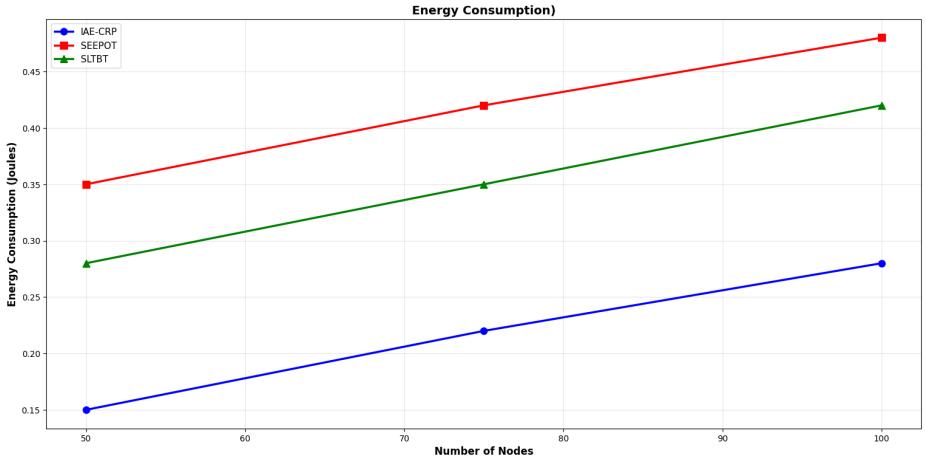

Figure 4: Energy Consumption

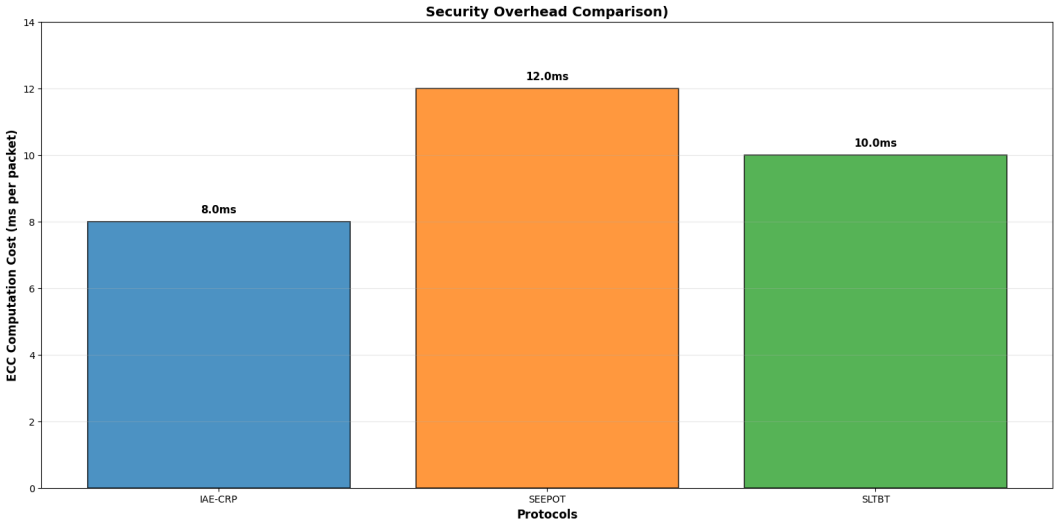

Figure 5: Security Overhead Comparison

TABLE II
Comparative analysis

Parameter	IAE-CRP	SEEPOT	SLTBT
Network throughput (Kbps)	534.87	242.1	119.5
Packet Delivery Ratio (%)	96.87	82.51	87.65
Energy Consumption (Joules)	0.15	0.35	0.28
Security Overhead (ms)	8.0	12.0	10.0

VII. CONCLUSION

The major drawback of WSN is that it consumes more energy during the communication process within the network. In order to overcome this issue, we introduced a routing protocol, namely the Improved Ant Optimisation with ECC mechanism-based Clustered Routing Protocol, which mainly concentrates on both energy efficiency and security enhancement in the network. Our protocol performs better when compared with the earlier protocols, such as SEEPOT and SLTBT. However, this model is not suitable for applications with critical faults because it lacks a fault tolerance mechanism. The IAE-CRP protocol surpasses SEEPOT and SLTBT in wireless networks with a throughput of 534.87 Kbps — notably higher than SEEPOT's 242.1 Kbps and SLTBT's 119.5 Kbps. It also achieves a packet delivery ratio of 96.87%, an enhancement over SEEPOT's 82.51% and SLTBT's 87.65% despite wormhole attacks. IAE-CRP's energy consumption of 0.15 Joules is significantly lower compared to SEEPOT and SLTBT, reducing it by 57% and 46%, respectively, prolonging network lifespan. Security overhead is reduced to 8.0 ms with the use of ECC-based key generation and ACO path optimisation, much lower than SEEPOT's 12.0 ms and SLTBT's 10.0 ms. Future research on the IAE-CRP method could explore adding fault tolerance for real-time IoMT applications and scaling up for larger wireless sensor networks. Combining ACO with machine learning, like LSTM, could improve predictions of evolving network topologies and routing efficiency.

FUNDING

This work was supported by the International Applied and Theoretical Research Center (IATRC), Baghdad, Iraq [grant number IATRC/2024/ENG/021].

ACKNOWLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] S.M.K.M. Abbas Ahmad, E. Krishnahari, et.al, "Neighbour node intimacy (N2i) for trust management in WSN", ELSEVIER - Materials Today: Proceedings, 2020.
[2] Anita Daniel D, S. Emalda Roslin, et.al, "Data validation and integrity verification for trust-based data aggregation protocol in WSN", ELSEVIER - Microprocessors and Microsystems, 2020.
[3] Nageswar Rao, B. Rajendra Naik and L. Nirmala Devi, "On the relay node placement in WSNs for lifetime maximisation through metaheuristics", ELSEVIER - Materials Today: Proceedings, 2020.
[4] D. Gopika and Rukmani Panjanathan, "Energy efficient routing protocols for WSN-based IoT applications: A review", 'ELSEVIER - Materials Today: Proceedings', 2020.
[5] Ilhem Souissi, Nadia Ben Azzouna and Lamjed Ben Said, "A multi-level study of information trust models in WSN-assisted IoT", ELSEVIER - Computer Networks, Vol. 151, pp. 12-30, 2019.
[6] Wen Li and Sami Kara, "Methodology for Monitoring Manufacturing Environment by Using Wireless Sensor Networks (WSN) and the Internet of Things (IoT)", 'ELSEVIER - 24th CIRP Conference on Life Cycle Engineering', vol. 61, pp. 323-328, 2017.
[7] Manu Elappila, Suchismita Chinara and Dayal Ramakrushna Parhi, "Survivable Path Routing in WSN for IoT applications", 'Pervasive and Mobile Computing', 2017.
[8] Renato F. Fernandes Jr and Dennis Brandao, " Proposal of Receiver-Initiated MAC Protocol for WSN in urban environment using IoT ", ELSEVIER – IFAC Conference, vol. 49, no. 30, pp. 102-107, 2016.
[9] Sangdae Kim, Cheonyong Kim and Kwansoo Jung, "Cooperative multipath routing with path bridging in wireless sensor network toward IoTs service", ELSEVIER- Ad Hoc Networks, vol. 106, 2020.
[10] Aparna Ashok Kamble and B.M. Patil, "Systematic analysis and review of path optimisation techniques in WSN with mobile sink", ELSEVIER-Computer Science Review, vol. 41, 2021.
[11] WALID OSAMY, AHMED A. EL-SAWY AND AHMED SALIM, "CSOCA: Chicken Swarm Optimisation Based Clustering Algorithm for Wireless Sensor Networks", 'IEEE ACCESS', vol. 8, 2020.

[12] Etobi Damian Tita and Williams-Paul Nwadiugwu," Real-time optimisations in energy profiles and end-to-end delay in WSN using two-hop information", 'Computer Communications', vol. 172, pp. 169-182, 2021.
[13] S.M. Mahdi H. Daneshvar, Pardis Alikhah Ahari Mohajer and Sayyed Majid Mazinani, "Energy-Efficient Routing in WSN: a Centralised Cluster-Based Approach via Grey Wolf Optimiser", IEEE ACCESS, vol. 8, 2017.
[14] Vinitha, M.S.S. Rukmini and Dhirajsunehra, "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimisation algorithm", 'Journal of King Saud University –Computer and Information Sciences', 2019.
[15] Amir Seyyedabbasi and Farzad Kiani, "MAP-ACO: An efficient protocol for multi-agent path finding in real-time WSN and decentralised IoT systems", 'Microprocessors and Microsystems', vol. 79, 2020.
[16] MOHAMMED FARSI, MAHMOUD BADAWY, et.al, "A Congestion-Aware Clustering and Routing (CCR) Protocol for Mitigating Congestion in WSN", 'IEEE ACCESS', vol. 7, 2019.
[17] Kalaivanan Karunanithy and Bhanumathi Velusamy, "Cluster-tree based energy efficient data gathering protocol for industrial automation using WSNs and IoT", 'Journal of Industrial Information Integration', vol. 19, 2020.
[18] HASSAN EL ALAMI AND ABDELLAH NAJID, "ECH: An Enhanced Clustering Hierarchy Approach to Maximise Lifetime of Wireless Sensor Networks", 'IEEE ACCESS', vol. 7, 2019.
[19] Alessandro Di Stefano, Aurelio La Corte, et. al, "It measures like me: An IoTs algorithm in WSNs based on heuristics behaviour and clustering methods", ELSEVIER - Ad Hoc Networks, vol. 11, pp. 2637-2647, 2013.
[20] ZHIDONG ZHAO, DUOSHUI SHI, et.al, "An Energy-Optimisation Clustering Routing Protocol Based on Dynamic Hierarchical Clustering in 3D WSNs", IEEE ACCESS, vol. 7, 2019.
[21] K. Thangaramya, K. Kulothungan, et.al, "Energy Aware Cluster and Neuro-Fuzzy Based Routing Algorithm for Wireless Sensor Networks in IoT", 'Computer Networks', 2019.
[22] Ramya Kulandaivel, S.Periyanayagi and S.Susikala, "Performance Comparison of WSN WSAN using Genetic Algorithm", 'International Conference on Communication Technology and System Design' vol. 30, pp. 107-112, 2012.
[23] Ming Tao, Xueqiang Li, et.al, "UAV-Aided trustworthy data collection in federated-WSN-enabled IoT applications", 'Information Sciences', vol. 532, pp. 155-169, 2020.
[24] Sachin Sen and Chandimal Jayawardena, "Reliability and Cybersecurity Improvement Strategies in Wireless Sensor Networks for IoT-enabled Smart Infrastructures", 'Global Conference for Advancement in Technology (GCAT)', pp. 18 to 20, 2019.
[25] Divya R. and Dr R.Chinnaiyan, "Reliable Constrained Application Protocol to Sense and Avoid attacks in WSN for IoT Devices", 'International Conference on Communication and Electronics Systems', 2019.
[26] N.Prakash, Dr M.Rajalakshmi and Dr R. Nedunchezhian, "ANALYSIS OF QoS FOR CONVEYING AUTHORISATION BASED ON INTERNET OF THINGS (IOT) IN WIRELESS SENSOR NETWORKS (WSN)", 'International Conference on Smart Structures and Systems ICSSS', 2020.
[27] S. A. M. Ali and E. H. Al-Hemairy, "Minimising E2E Delay in V2X over Cellular Networks: Review and Challenges," Int. J. Inf. Commun. Technol., vol. 3, no. 2, pp. 18–26, Dec. 2019. [Online]. Available: https://ijict.edu.iq/index.php/ijict/article/view/79.
[28] S. R. Al-Hafidh and E. H. Al-Hemiary, "Simplified Distributed Ledger for Task Offloading in Edge Networks," Int. J. Inf. Commun. Technol., vol. 6, no. 1, pp. 35–44, Dec. 2024. [Online]. Available: https://ijict.edu.iq/index.php/ijict/article/view/247.
[29] R. Uddin, T. Hwang, and I. Koo, "Worker Presence Monitoring in Complex Workplaces Using BLE Beacon-Assisted Multi-Hop IoT Networks Powered by ESP-NOW," Electronics , vol. 13, no. 21, p. 4201, Oct. 2024, doi: 10.3390/electronics13214201.
[30] T. Y. Obaid and A. A. Kadhim, "Modified RPL Routing Protocol for Dense IoT Networks," Int. J. Inf. Commun. Technol., vol. 7, no. 3, pp. 1–17, Dec. 2024. [Online]. Available: https://ijict.edu.iq/index.php/ijict/article/view/219.
[31] B. Clerckx et al. , "Multiple Access Techniques for Intelligent and Multifunctional 6G: Tutorial, Survey, and Outlook," Proceedings of the IEEE , vol. 112, no. 7, p. 832, Jun. 2024, doi: 10.1109/jproc.2024.3409428.
[32] M. S. Abood, H. Wang, D. He, M. Fathy, S. A. Rashid, M. Alibakhshikenari, B. S. Virdee, S. Khan, G. Pau, I. Dayoub, P. Livreri and T. A. Elwi, "An LSTM-Based Network Slicing Classification Future Predictive Framework for Optimised Resource Allocation in C-V2X," IEEE Access, vol. 11, pp. 129300-129310, 2023, doi: 10.1109/ACCESS.2023.3332225.

