Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol.44 No. 6 (2023)

Location Based Energy Efficient Security Mechanism in Wireless Sensor Networks using Trust Aware Localized Key Management Technique

[1]Sudhakar Avareddy , [2]Rajashree V Biradar , [3]V.C.Patil, [4]Namratha V Patil

Dept. Of CSE Ballari Institute of Technology &Management India Ballari

JSS Science and TechnologyUniversity Mysore, India

***Abstract*—**Wireless Sensor Networks (WSNs) have gained significant popularity applications in a variety of fields, including as environmental monitoring, healthcare, and security surveillance, are possible. However, ensuring the security of WSNs remains a formidable challenge due to resource constraints and the dynamic nature of these networks. In response, location-based security management has emerged as a promising approach to bolster WSN security by leveraging node location information to mitigate potential threats. This paper presents a novel trust aware localized key management technique known as TrustAware-QL-PSO-AES algorithm that integrates Trust awareness to a hybrid Qlearning-PSO-AES algorithm, offering an effective and energy-efficient trust aware location-based security mechanism for WSNs.The proposed technique encompasses essential components, such as location information, dynamic trust evaluation, and advanced encryption algorithms, to significantly enhance the security of WSNs. The Qlearning algorithm plays a central role in learning the current state of each node, including its position and velocity, while simultaneously estimating trust values based on past interactions. Concurrently, the PSO algorithm optimizes the placement of sensor nodes within the network, effectively enhancing network lifetime, coverage, connectivity, and energy consumption.Moreover, the PSO algorithm's optimal solution, represented by the best fitness value, is utilized for selecting encryption keys in the AES algorithm. These encryption keys are dynamically updated based on node movement, providing an additional layer of security to WSNs. Proposed technique embraces a trust-aware concept, ensuring that data packets are routed through trusted nodes, further reinforcing the overall security framework.Extensive simulation results illustrate the efficacy of proposed Trust Aware Localized Key Management Technique, which not only significantly enhances the security of WSNs but also demonstrates remarkable efficiency in optimizing network performance. As a result, this approach proves to be well-suited for real-world applications across various domains, where both security and energy efficiency are critical considerations.

Keywords: *Wireless Sensor Networks, Location-based Security, Trust Aware Localized Key Management, Qlearning, PSO, Advanced Encryption Standard.*

Introduction

Wireless Sensor Networks (WSNs) have become indispensable in a variety of applications, including as industrial automation, smart cities, healthcare, and environmental monitoring [1]. These networks are made up of lots of tiny, low-power sensor nodes that can sense, process, and transmit data to a central node or sink as shown in Fig.1 [1]

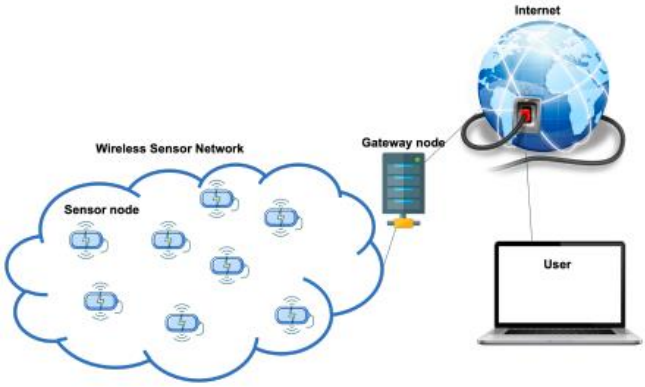

Fig.1: Sensor network communication architecture[15]

However, the distributed and resource-constrained nature of WSNs poses significant challenges in terms of security, energy efficiency[2], and scalability [3,12].Ensuring the security of data transmission in WSNs is of utmost importance, as these networks often operate in unattended and hostile environments. The limited computational capabilities of sensor nodes make it challenging to implement traditional encryption algorithms for secure communication. Moreover, the broadcast nature of wireless communications [4] exposes WSNs to a variety of security concerns, including denial-of-service attacks, unauthorized access, and data manipulation. Location-based security management has emerged as a promising approach to enhance the security of WSNs. By leveraging the spatial information of sensor nodes, location-based mechanisms can effectively detect and mitigate security threats. Additionally, incorporating energy-efficient solutions is vital to extend the network's lifetime and reduce operational costs.

In this paper, proposed Trust Aware Localized Key Management algorithm (TrustAware-QL-PSO-AES) for WSNs. The proposed technique combines the strengths Trust Awareness, Qlearning, (PSO) Particle Swarm Optimization, and Advanced Encryption Standard (AES) algorithm. The Qlearning algorithm enables the nodes to learn their current state, including position and velocity, and to estimate trust values based on past interactions. PSO optimizes the placement of sensor nodes, improving network coverage, connectivity, and energy consumption. AES ensures secure communication by dynamically updating encryption keys based on node movements.

The key contributions of the work are:

1. A hybrid Qlearning-PSO-AES algorithm for location-based security management, providing enhanced data confidentiality and integrity.

2. Incorporation of the Trust Aware Localized Key Management Technique to evaluate dynamic trust levels and adapt encryption keys accordingly.

3. Demonstration of improved energy efficiency and network performance through extensive simulations.

The rest of the paper is organized as follows: Section II provides an overview of related work in the field of WSN security and energy efficiency. Section III details the proposed Location-Based Energy Efficient Security Mechanism, including the Trust Aware Localized Key Management Technique. Section IV presents the simulation setup and evaluation results. Finally, Section V concludes the paper and discusses future research directions for the advancement of WSN security and efficiency.

Related work

In this section discussed the related techniques of proposed TrustAware-QL-PSO-AES algorithm which includes localization, security, Qlearning and trust management techniques.

1. Localization

The localization of sensor nodes, or the determination of node placements in the target region, represents one of the major challenges in achieving energy efficiency. Comparison of various localization techniques [5] proves

clearly that PSO is the best algorithm for optimizingthe position of the sensor nodes. PSOalgorithm is globally adapted as a high-performance optimization tool.

Table I gives comparison of localization methods that are currently used and based on analysis; it is found that PSO is the best localization algorithm.

TABLE I COMPARISON OF VARIOUS LOCALIZATION TECHNIQUES [6]

Methods	*Expenditure*	*Precision*	*Energy Consumption*	*Hardware Size*
Include GPS	Additional Amount	Max	Low	Large
Exclude GPS	Less	Avg	Medium	Small
Centralized	Based On Type	Max	Low	Based On Type
Decentralized	Based On Type	Min	High	Based On Type
Angle Of Arrival	Additional Amount	Min	Medium	Large
Time Of Arrival	Additional Amount	Avg	Low	Large
RSSI	Less	Avg	High	Small
PSO	Less	Max	High	Small

The basic idea of PSO [8] is to simulate the social behavi of a swarm of particles, where each particle represents a possible solution to the optimization problem. Each particle in the swarm has a position and velocity in the solution space. The position of a particle represents a potential solution to the problem, and the velocity determines the direction and magnitude of the movement of the particle in the solution space. The PSO [9] algorithm iteratively updates the position and velocity of each particle based on its own best position (pbest) and the best position of the swarm (gbest).

$$v\_i(t+1) = w * v\_i(t) + c1 * r1 * (pbest\_i - x\_i(t)) + c2 * r2* (gbest - x\_i(t)) \quad (1)$$

$$x\_i(t+1) = x\_i(t) + v\_i(t+1) \quad (2)$$

Wherev_i(t) is the velocity of particle i at time t, x_i(t) is the position of particle i at time t, pbest_i is the best-known position of particle i, gbest is the best-known position among all particles, w isthe inertia weight, c1 and c2 are the acceleration constants, and r1 and r2 are random numbers between 0 and 1.

The flowchart for the particle swarm optimization algorithm's target localization technique is shown in Fig. 2 [7]. In the wireless sensor network depicted in Fig. 2, target points were produced at random inside a 100 m square. With random numbers, its starting velocity creates a two-dimensional matrix with a range of [-1, 1]. After a number of motions, the particle swarm is compared to one another, and the particle swarm proceeds in the direction with the highest fitness value until the predetermined stopping condition is met. The estimate point is thought of as being in the position that corresponds to the most recent global optimal solution. Additionally, inertia weight is introduced to the PSO algorithm's target localization technique [10] to boost effectiveness..

Table Ii. Properties Of The Encryption Algorithms.[14]

Algorithm	Security level	Efficiency	Scalability	Computational overhead	Key length
AES	High	High	Medium	Low	128 bits 192 bits 256 bits
DES	Moderate	High	Medium	Low	56 bits
RSA	High	Low	Low	High	Variable
ECC	High	High	High	Low	Variable

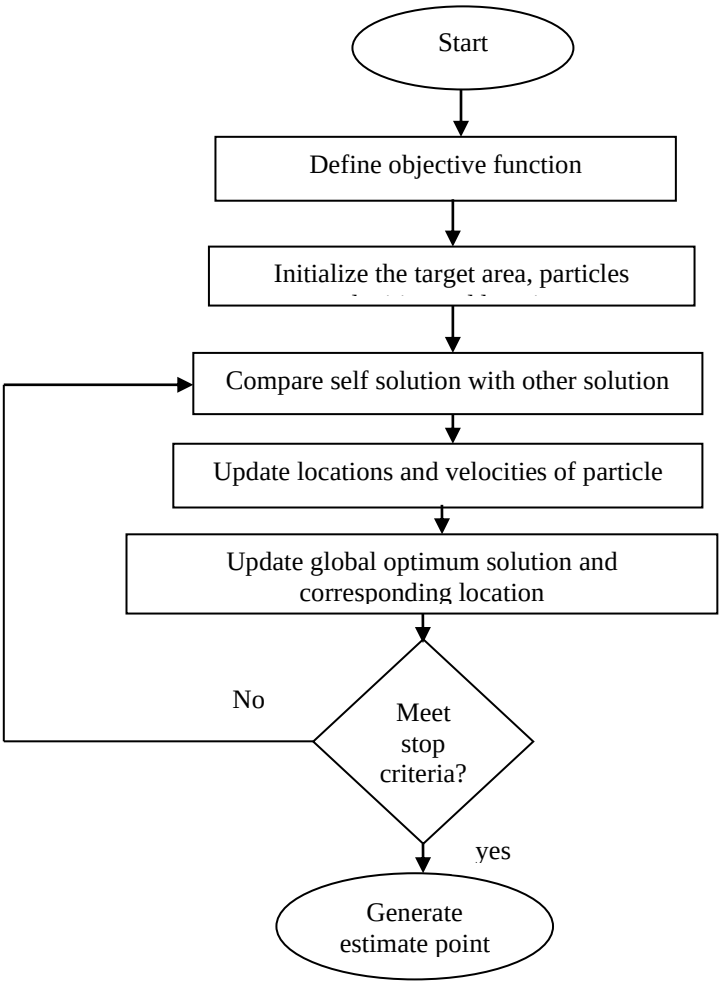

Fig 2. Flow chart of PSO

2. Security

Table II gives the Information on the comparison study of the WSN's existing security methods.The Advanced Encryption Standard (AES) is the finest security mechanism, according to the comparative analysis, because of its long block length and a variety of key lengths.

The Data Encryption Standard (DES) algorithm was replaced with the symmetric block cipher known as the AES. Three alternative key lengths can be used with the widely used and standardised AES cipher: 128 bits, 192 bits, and 256 bits..

These days, AES is widely used. For AES, many libraries have been created in a variety of computer languages, including C, C++, Java, and Python. These days, even Facebook and WhatsApp employ AES to protect the confidentiality of transmitted messages.There are numerous hardware implementations for AES operations in Intel and AMD CPUs as a result of how standardised it is.

In Fig.3 [15] described security of the communication when it is assumed that only the sender and the receiver have access to and are aware of the symmetric shared key.

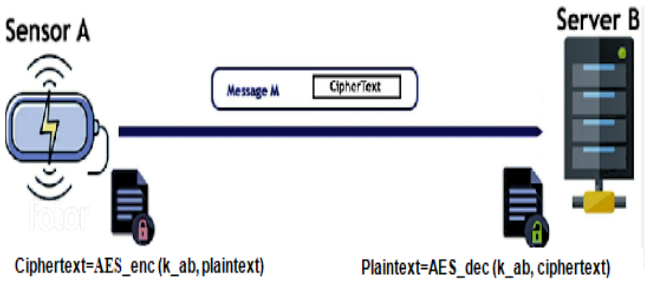

Fig 3. AES sent packet.

3. Q-learning

This section gives details of Q-learning algorithm.[12] Q-learning is a reinforcement learning algorithm used in machine learning and artificial intelligence to solve problems where an agent interacts with an environment to achieve a goal.

Key Components:

✓ **Agent:** The entity or system that makes decisions and learns from its interactions with the environment.
✓ **Environment:** The external system or environment that the agent communicates with based on the agent's behaviors, it delivers feedback..
✓ **State (s):** An illustration of the environment's current state or set up. The agent makes decisions based on this data..
✓ **Action (a):** The range of actions an agent may make in a specific condition.
✓ **Reward (r):** After each action, the environment gives the agent a numerical value. It reveals how effective or ineffective the action was in that specific situation.
✓ **Policy (π):** A strategy or set of rules that the agent uses to determine which action to take in each state.

$$Q(s, a) \leftarrow Q(s, a) + \alpha[R + \gamma \max Q(s0 , a 0) - Q(s, a)] \quad (3)$$

where is the learning rate, which ranges from 0 to 1. R is a reward and represents the pace at which the reward is reduced over time.The action's Q-value for the current state is Q (s, a). The equation that determines the optimum course of action in the present condition is added to the existing value Q (s, a) and S to update it. By continually updating the Q-value for each state using the equation (3) above. Rewards are offered before Q-learning even starts on the Q-table. If an agent chooses an action through a policy in the first state, it enters the subsequent state. This procedure is done numerous times when using the Q-table to solve a specific problem until the overall Q-value converges to a specific value.

4. Trust Management Technique.

Trust management is essential for maintaining the security and dependability of data transmission and node collaboration in wireless sensor networks. The term "trust" refers to the degree of assurance and significance given to each node in a sensor network. There are basically two types of trust management schemes: centralised trust management and distributed trust management. In a centralized trust management scheme, there is a central authority or trust manager that is responsible for monitoring and evaluating the trustworthiness of all nodes in the network.Distributed trust management schemes, on the other hand, rely on a decentralized approach where trust-related information is distributed among all nodes in the network.Nodes in a WSN maintain their trust-related data, such as reputation scores and observed behaviors of neighboring nodes.Comparison Of various Trust Management Schemes Based On Security Metrics is given in Table III.

Table Iii. Comparison Of Trust Management Schemes Based On Security Metrics [6]

Trust Management Scheme	**Trust Assessment Basis**	**Complexity**	**Overhead**	**Resilience to Attacks**
Node Reputation-Based	Past Behavior, Interactions	Moderate	Moderate	Limited
Behavior-Based	Observed Behavior	Moderate	Moderate	Limited
Energy-Based	Energy Consumption Patterns	Low to Moderate	Low	High
Security Metrics-Based	Cryptographic Measures, Protocols	High	High	Moderate
Anomaly Detection-Based	Anomalies, Deviations	High	High	High

I. PROPOSED WORK

Lack of security, more energy consuming & less efficiency and limited trust management are some of the limitations of existing models. All these limitations are addressed in this proposed work. The proposed work involves implementation of Location Based Energy Efficient Security Mechanism in Wireless Sensor Networks using Trust Aware Localized Key Management Technique.

In the proposed TrustAware-QL-PSO-AES algorithm, each sensor node maintains a trust level that reflects its reliability and trustworthiness within the network. This trust level is dynamically updated based on the node's behavior, interactions, and performance. Nodes that consistently exhibit secure and efficient behavior are rewarded with higher trust levels, while nodes engaging in suspicious or energy-inefficient activities receive lower trust levels.

$$Trust\_Level(Node\_i, t+1) = Trust\_Level(Node\_i, t) + \alpha * (Reward(Node\_i, t) - Penalty(Node\_i, t)) \quad (4)$$

Trust_Level (Node_i, t+1): Trust level of Node_i at time t+1.

Trust_Level (Node_i, t): Trust level of Node_i at time t.

α: Trust update rate or learning rate (a parameter controlling the rate of trust adjustment).

Reward (Node_i, t): Reward obtained by Node_i at time t based on secure and efficient behavior.

Penalty (Node_i, t): Penalty imposed on Node_i at time t for any suspicious or inefficient behavior.

The above equation reflects a trust update mechanism, where nodes increment their trust levels when they exhibit positive behavior (receiving rewards) and decrement them when displaying negative behavior (incurring penalties). Over time, this trust-awareness mechanism helps nodes make decisions that prioritize interactions with trusted neighbors and avoid unreliable or potentially malicious nodes.

The implementation steps of hybrid TrustAware-QL-PSO-AES algorithm for location-based security management in Wireless Sensor Networks are as follows.

i. Initialize the WSN: Set up the WSN by deploying sensor nodes in the target area and establish communication links between them.
ii. Define the objective function: Based on problem defined for optimizing energy consumption, coverage, connectivity and network lifetime.
iii. Initialize Parameters: Define the necessary parameters such as the number of particles, maximum iterations, learning rate (alpha), discount factor (gamma), exploration rate (epsilon), initial energy level, and energy threshold.
iv. Initialize Q-table: Create a Q-table with dimensions corresponding to the number of particles and the total number of actions (2 * number of dimensions).
v. Initialize each node with Trust Table to maintain trustiness value of its neighboring nodes.
vi. Initialize a swarm of particles with random positions and velocities within the network boundaries.
vii. Evaluate the fitness of each particle based on required objective function.
viii. Select an action for each node using the Q-learning algorithm. Choose either exploration (random action) or exploitation (action with the highest Q-value).
ix. Calculate the global best position, global best fitness value.
x. Evaluate the trust values of neighboring nodes using trust evaluation metrics.
xi. Assign the trust values to nodes based on their fitness value, their past interactions and evaluations.
xii. Calculate the reward for the interaction between the node and its neighbor based on the trust value.
xiii. Update the Q-table using the Q-learning update equation, incorporating the reward and the maximum future Q-value.
xiv. Update the node's position and velocity based on the selected action.
xv. Use the optimal solution obtained to select encryption keys for the AES algorithm.
xvi. Update the encryption keys dynamically as per the node movement to enhance the security of the WSN.
xvii. Repeat steps vii-xvi.
xviii. Develop a trust-based routing scheme that directs data packets through trusted nodes, considering their trust values and network topology.

Conduct simulations and experiments to evaluate the performance of the proposed technique in terms relevant metrics like security, energy efficiency, network lifetime, coverage, efficiency, and scalability. Compare the results with existing techniques to demonstrate the effectiveness of this approach.

Fig.4 depicts the flowchart for implementing the proposed a hybrid TrustAware Qlearning-PSO-AES key management algorithm.

Results And Discussion

Simulations were performed using python IDE (Pycharm) to evaluate the performance of the proposed algorithm. Simulations are run using different parameter settings that leads to the optimal solution. The simulation parameters provided in Table IV define the specific characteristics and constraints of the wireless sensor network (WSN) for the proposed TrustAware Qlearning-PSO-AES algorithm.

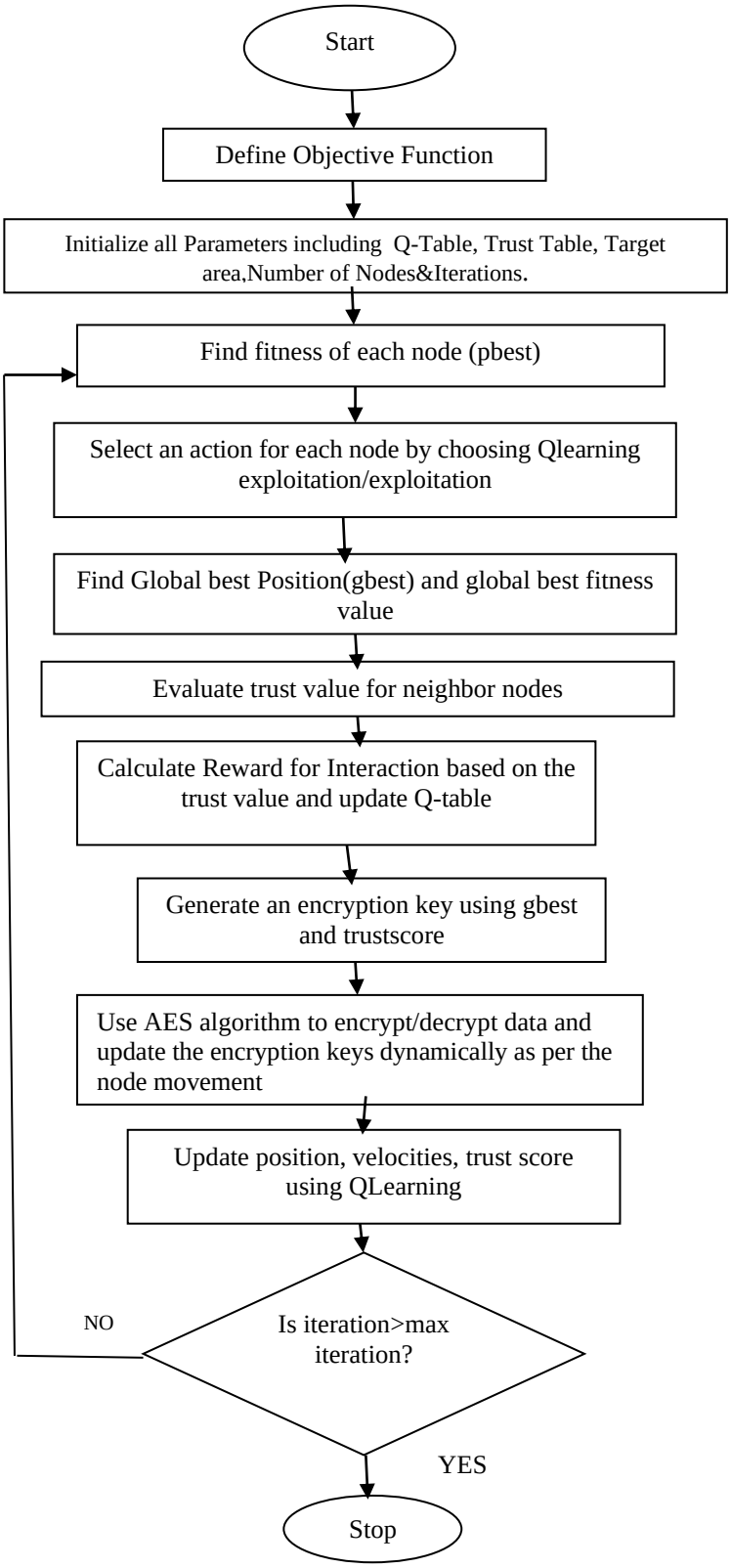

Fig.4. Flow diagram TrustAware Qlearning-PSO-AES key management algorithm

Table Iv: Simulation Parameters[11]

Target Area	100m*100m
Sensor Nodes	10,20,30,40,50,60
Maximum Iterations,	100,150,200,250,300,350
Learning Rate (Alpha),	0.1
Discount Factor (Gamma),	0.9
Exploration Rate (Epsilon),	0.1
Transmission range	10m
Energy Threshold.	5J
Data packet	1024 bits
Transmission energy	0.1J
Receiving energy	0.1J
Idle energy	0.05J
Encryption Key Size	256
C1(Cognitive constant)	1
C2(Social constant)	1
W	0.5
r1,r2	Random number between 0 to 1

In this proposed approach simulations arecarried out by varying the number of nodes from 10-60 to verify the ability to handle computational complexity. In order to improve performance, simulations are also run with iterations ranging from 100 to 350.

A. Results& Analysis

Simulation results are analyzed to understand the performance of the proposed approach using the following performance metrics.

- Scalability: It describes how well the proposed method can manage growing data volumes without noticeably degrading its performance.
- Convergence speed: It indicates the speed at which the algorithm achieves the desired or optimal outcome.

- Energy consumption: The total energy utilized during the computational and communication processes in order to arrive at the desired solution
- Efficiency: It evaluates how well the trade-off between scalability, computational complexity, and solution quality is balanced.

The results obtained by altering the number of nodes from 10 to 60 are displayed in Fig.5 to 8.

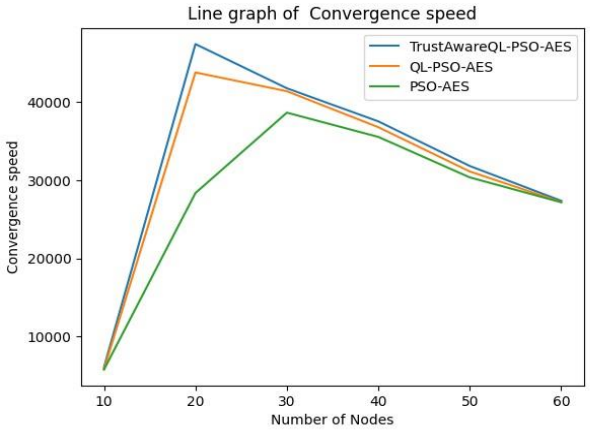

Fig.5. Number of Nodes v/s Convergence speed

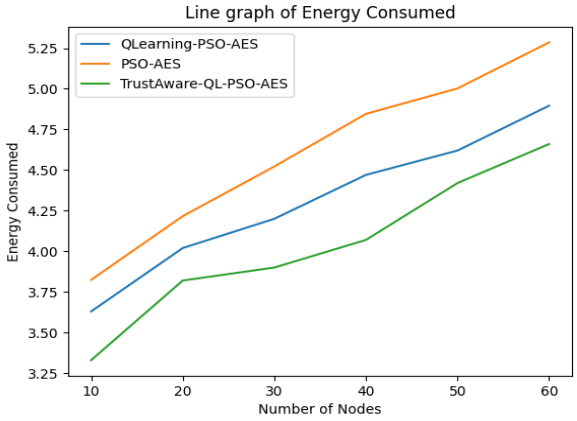

Fig. 6.Number of Nodes v/s Energy consumed

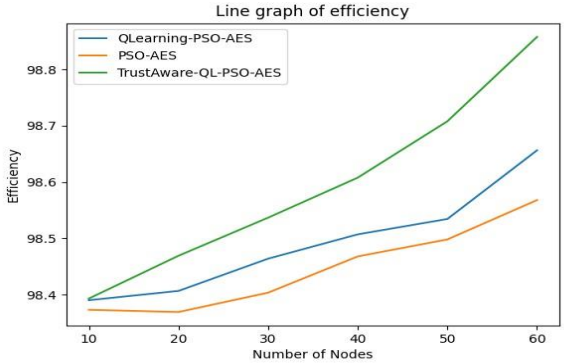

Fig.7. Number of Nodes v/s Efficiency

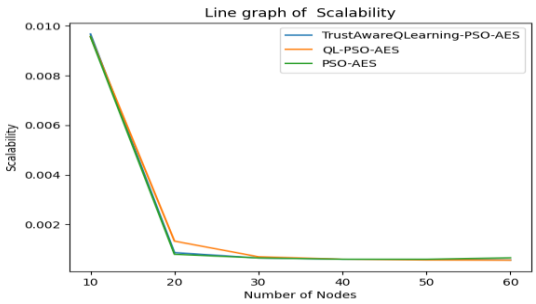

Fig.8.Number of Nodes v/s Scalability

In the Proposed TrustAware-QL-PSO-AES algorithm, as the number of nodes increases, Efficiency decrease and Energy Consumption increases due to various factors like communication overhead, collisions and interference, trust evaluation overhead, data aggregation challenges and resource constraints. As the number of nodes increasesConvergence Speed and Scalability diminishes for a variety of reasons including increased communication costs, lack of global knowledge and coordination,resource limitations and synchronization issues.

TrustAware-QL-PSO-AES algorithm outperforms compared to QLearning-PSO-AES and PSO-AES as it uses trust model to evaluate the trustworthiness of nodes in the network and it additionally, integrates trust evaluations into the decision-making processes. Trust-aware variants are particularly valuable in scenarios (adversarial or unreliable environments) where trustworthiness and security are paramount, but they may introduce additional overhead.

Fig. 9 through Fig. 12 displays the outcomes of using different iterations between 100 and 350.

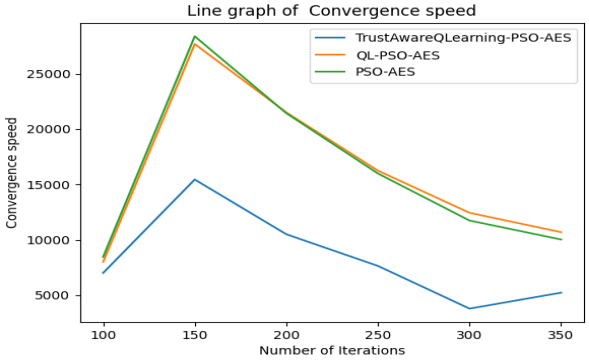

Fig.9. Number of Iterations v/s Convergence speed

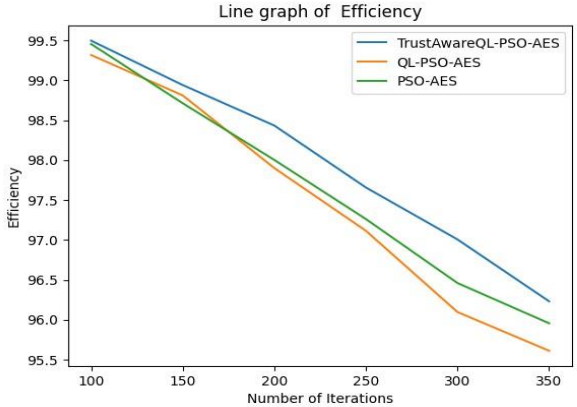

Fig.10. Number of Iterations v/s Efficiency

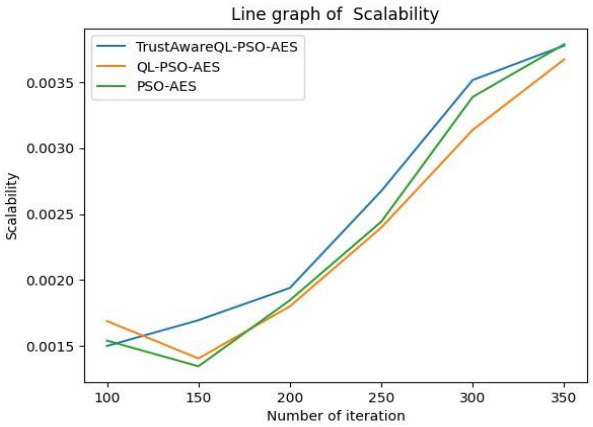

Fig.11. Number of Iterations v/s Scalability

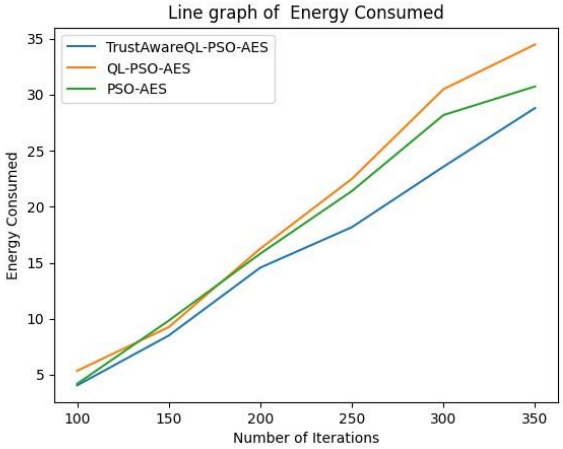

Fig.12.Number of Iterations v/s Energy consumed

As the number of iterations increases the efficiency decreases and energy consumed increases due to factors such as the communication overhead, computational complexity, algorithm convergence rate, resource constraints, dynamic network conditions. As the number of iterations increases,this algorithm typically converges to a solution more quickly when it starts with fewer iterations. In other words, it completes the task more quickly and to a good outcome. This is especially true for algorithms that engage in exploration and exploitation, like reinforcement learning, where first iterations examine several possibilities. As the number of iterations rises, scalability initially decline. The algorithm can improve its performance or converge towards a better result with increasing iterations.With increasing iterations, the algorithm has more opportunities to fine-tune its parameters, learn from data, and explore a broader solution space. This can result in improved performance and the discovery of more optimal solutions.

TrustAware-QL-PSO-AES algorithm outperforms with the increasing iterations because trust-awareness allows nodes to make more informed and adaptive decisions.Trust evaluations help nodes identify trustworthy neighbors and avoid unreliable ones, which can lead to quick optimal solution in dynamic environments.

Conclusion and Future scope

The proposed TrustAware-QL-PSO-AES algorithm, presents a novel approach for location-based security management in Wireless Sensor Networks. By harnessing the collective strengths of Qlearning, Particle Swarm Optimization and Advanced Encryption Standard algorithm, this technique addresses the limitations of existing approaches while offering numerous advantages. Through the synergistic combination of Trust awareness, Qlearning, PSO, and AES, algorithm significantly enhances the optimization process, resulting in improved security, energy efficiency, extended network lifetime, and enhanced coverage in WSNs. Moreover, the

integration of AES encryption adds a robust layer of security to data transmission, safeguarding sensitive information from unauthorized access and ensuring data integrity. The results of extensive simulations validate the effectiveness of this approach, demonstrating notable improvements in both security and energy efficiency. By leveraging trust-awareness and intelligent localization, the proposed mechanism offers a well-rounded solution for the challenges posed by security and energy management in WSNs.

Currently, the trust evaluation is based on past interactions. Future extensions can integrate real-time feedback and dynamic trust assessment mechanisms, taking into account changing node behaviors and network conditions.Using advanced machine learning algorithms can also enhance the trust evaluation process by predicting the future trustworthiness of sensor nodes based on historical data. Incorporating sophisticated machine learning methods, such as Deep Reinforcement Learning (DRL).with TrustAware-QL-PSO-AES algorithm, it is possible to significantly enhance its decision-making and trust evaluation capabilities in dynamic and complex Wireless Sensor Network (WSN) environments.

References

[1] Sai Krishna Kovi, Pavankumar Jangam, Sai Kumar Goud Kosg:"WirelessSensorNetworksAndApplications" publication at:https://www.researchgate.net/publication/317798885 June 2017.

[2] Mamoona Majid Shaista Habib Abdul Rehman Javed MuhammadRizwanGautamSrivastava,ThippaReddyGadekalluandJerryChun-Wei Lin, "Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: Systematic Literature Review", Published online 2022 Mar.

[3] Elhadi Shakshukia, Abdulrahman Abu Elkhailb, Ibrahim Nemerb,MuminAdamb,TarekSheltamib,"ComparativeStudyonRangeFreeLocalization Algorithms", The 10th International Conference on Ambient Systems, Networks and Technologies(ANT) April29-May2,2019.

[4] Shweta Singh, Ravi Shakya, Yaduvir Singh, "Localization Techniques in Wireless Sensor Networks", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6(1), 2015, 844-850.

[5] D. Moore, J. Leonard, D. Rus, and S. Teller, "Robust distributednetwork localization with noisy range measurements",Proceedings ofthe Second ACM Conference on Embedded Networked SensorSystems (SenSys '04), Baltimore, MD, pp. 50-61, November 2004.

[6] Sudhakar Avareddy and RajashreeV.Biradar, "Comparative AnalysisofLocalizationTechniquesandSecurityMechanismsinWSN",IEEEInternational Conference on Mobile Networks and WirelessCommunications (ICMNWC), 3rd - 4th Dec. 2021, at Tumkur,Karnataka,India

[7] Shu-Hung Lee , Chia-Hsin Cheng ,Chien-Chih Lin and Yung-Fa Huang ," PSO-Based Target Localization and Tracking in Wireless Sensor Networks" Electronics 2023, 12, 905. https://doi.org/10.3390/electronics12040905 https://www.mdpi.com/journal/electronics

[8] Satinder Singh Mohar,Sonia Goyal,Ranjit Kaur,"Localization of sensor nodes in wireless sensor networks using bat optimization algorithm with enhanced exploration and exploitation characteristics" The Journal of Supercomputing (2022)78:11975–12023 https://doi.org/10.1007/s11227-022-04320-x.

[9] Cen Cao, Qingjian Niand, Xushan Yin," Comparison of Particle Swarm Optimization Algorithms in Wireless Sensor Network Node Localization" 2014 IEEE International Conference on Systems, Man, and Cybernetics October 5-8, 2014, San Diego, CA, USA.

[10] Huanqing Cui , Minglei Shu ,Min Song and Yinglong Wang "Parameter Selection and Performance Comparison of Particle Swarm Optimization in Sensor Networks Localization" Sensors 2017,17,487; doi:10.3390/s17030487www.mdpi.com/journal/sensors.

[11] Qiaohe Yang," A new localization method based on improved particle swarm optimization for wireless sensor networks" © 2021 The Authors. IET Software published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

[12] Beakcheol Jang, Myeonghwi Kim,Gaspard Harerimana,And Jong Wook Kim," Q-Learning Algorithms: A Comprehensive Classification and Applications" VOLUME 7, 2019September 27, 2019. Digital Object Identifier 10.1109 /ACCESS .2019.2941229.

[13] Vikash Kumar , Anshu Jain and P N Barwal, Wireless Sensor Networks: Security Issues, Challenges and Solutions International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 859-868 © International Research Publications House http://www. irphouse.com.

[14] Murat Dener," Comparison of Encryption Algorithms in Wireless Sensor Networks" ITM Web of Conferences22,01005(2018),CMES-2018 https://doi.org/10.1051/itmconf/20182201005.

[15] Mauro Tropea, Mattia Giovanni Spina, Floriano De Rango and Antonio Francesco Gentile," Security in Wireless Sensor Networks: A Cryptography Performance Analysis at MAC Layer" Future Internet 2022, 14, 145. https://doi.org/10.3390/fi14050145 https://www.mdpi.com/journal/futureinternet.