SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V9I10P104

Volume 9 Issue 10, 19-26, October 2022
© 2022 Seventh Sense Research Group®

Original Article

A Novel Spider Swarm Optimized Energy and Security Aware Clustering Protocol for Smart Grid Wireless Sensor Network

Karpaga Priya R[1], Gayathri C[2], Ramela KR[3], S. Mahaboob Basha[4]

[1] *Department of EEE, Saveetha Engineering College, Chennai, India.*
[2] *Mother Teresa College of Engineering and Technology, Pudukkottai, India.*
[3] *Department of Electrical and Electronics Engineering, Ultra college of Engineering and Technology, Madurai, India.*
[4] *Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, India.*

[1]*Corresponding Author : coolpriya2296@gmail.com*

Received: 17 August 2022 Revised: 25 September 2022 Accepted: 08 October 2022 Published: 23 October 2022

Abstract **-** *The smart grid is a modern electric power grid infrastructure that uses brainy transmission and distribution networks to transport electricity. Using a wireless sensor network in a smart grid aims to increase the electric system's efficiency, reliability, and safety. In order to improve security, there is a lot of cryptography, authentication, and security mechanism was developed, but this was not enough to cope with attacks presented in the cluster. In order to overcome these attacks and enhance an energy-aware facility in the wireless Smart Grid, Spider Based Security and Energy Aware Clustering (SSEAC) are proposed in this paper. This proposed method focused on both Security and Energy consumption with three steps. Initially, the fuzzy-based clustering algorithm is presented to initialize the group of nodes for cluster formation. The second step carries the Trust Degree Evaluation of every individual node, which is one of the important security factors in fitness objective functions. Finally, the Spider Optimization Algorithm (SOA) is presented to find a Node Distance from a base station, the distance between the Node and Cluster Head (CH), total energy consumption, Received Signal Strength (RSS), and Node's Trust degree for optimum CH selection. In addition, this process may give a better result for highly secured data transmission. As a result, the proposed SSEAC method has a better outcome in the Network lifetime and Less Energy consumption with higher packet delivery rates than the prior methods.*

Keywords **-** *WSN, RSS, Smart grid, SSEAC, Spider optimization.*

1. Introduction

The smart grid is an advanced electric power grid communications utilizing intelligent broadcast and sharing networks to deliver power (Khurana *et al.*2010). The smart grid network is focused on developing the electricity's reliability, efficiency, and safety through modern technologies, dynamic optimization, automatic electric system control, safeguarding, and planning. The main sort of the electric power grid is automation and interaction, namely two-way communication of data consumption.

In smart grid communication, some of the challenges faced by the new generations are 1) congestion of network and safety concerns; (2) persistent lacking and successful communications, fault identification, monitoring, and automation; (3) integration of power grid, energy storage, stability, that are introduced by the renewable and different energy sources adaptation.

In the recent scenario, Wireless Sensor Networks (WSN) have been developed in all fields. Several sensors' nodes are arranged with the support of physical sources, namely humidity, temperature, acoustic and visual data. It is used to multimedia and sense scale data from an environment. These sensor nodes are interconnected wirelessly in WSNs Smart Grid applications which can team up for sense at low cost, collect, deliver, and process data in different fields like military applications, commercial purposes, environmental monitoring, robotics, etc.

The characteristic of the smart grid, which includes power transmission, power generation, distribution, substation, power utilization, and dispatch, WSN's security becomes a central concern. The WSNs security is not directly applied in Smart Grid because of its specific applications, and also, characteristics of sensor networks differ from other sensor networks. As a result, security is the main concern in smart grid systems, which may safeguard when the grid falls under attack. By considering attacks, the required security measures would be taken to prevent wireless attacks like jamming, eavesdropping by outside nodes, eavesdropping by malicious inside nodes, and launching security inside networks.

To solve all the attacks mentioned, many approaches have been developed to improve the security and lifetime of the Smart wireless grid. In this paper, the Spider Based Security and Energy Aware Clustering (SSEAC) is presented with the process of fuzzy clustering and Spider Optimization Algorithm (SOA), which enhances the results of Cluster Head selection with the advantages of less routing table size, increases the lifetime of the network, decreases the data packets redundancy and also mitigate the energy consumption value. On the other hand, the SSEAC focused on secured data transmission by implementing a Trust Degree Approach that evaluates the high trust degree of every individual node. Therefore the proposed SSEAC method is provided the best Security and Energy Aware with the comparison of previous methodologies.

The remainder of this paper is organized as follows. Section 2 illustrates the security issues in wireless smart grids. Section 3 addresses the related works based on the security and energy of wireless networks. Section 4 illustrates in the proposed SSEAC consists of clustering, CH selection based on objective functions, and SOA methods. Section 5 illustrates the experimental results, and Section 6 concludes the paper.

2. Security Issues in the Wireless Smart Grid

The Smart Grid wireless communications are facing a lot of troubles while data transmission and broadcasting are processed. Several security attacks are detected in the Wireless Sensor Node (WSN) and Wireless Mesh Network (WMN), making huge trouble for the Smart Grid. Some of the security issues of Wireless Smart Grid (WSG) are illustrated in the following.

- Jamming: This attack generates a malicious node purposely in the range of the same frequency band used in WSG. These attacks can be easily detected through signal detection.
- Eavesdropping by nodes outside Network: This attack is based on the malicious node that can access the network's data without authorization. This attack spies the details of packets sent in a WMN and may decrypt the packets of mesh nodes. This malicious node receives data without any signal emitting, which is more complex to detect the attack. A promising approach to this problem is to develop physical layer security techniques (Khurana *et al.*2015). To overcome these issues, the physical layer security is enabled where the eavesdropper cannot access any useful data even at the bit level, but this process possesses more computational power.
- Eavesdropping by malicious nodes inside the Network: It is caused by the legal node inside the network that does not follow security protocols or illegal nodes are bypassed as authenticated in a network. The malicious node passively gathers or spies packets' details when it does not conduct active security attacks. It has two variations of eavesdropping; firstly, the malicious node spies signals from other nodes. On applying physical layer security, the attacker node cannot decode signals from other nodes. Therefore, data encryption is protected the data flow secured in the smart grid. Next, the malicious node pretends to be a legal node and spies the packets from other nodes that are so complex to protect. This method analyzes the attacker node based on the receiving data patterns from other nodes.
- Launching security attacks by nodes inside the network. To begin security attacks, the attacker node requires being involved actively in network protocols. The attacker node can participate in routing and MAC protocols in the multi-hop network. A huge number of different attacks are launched: redirecting packets, dropping packets, contents of a packet changing, and disabling routing messages or ACKs MAC layer.

3. Related Works

Many researchers have applied clustering algorithms in WSN to achieve clustering efficiency with minimum computational complexity. Several clustering is based on artificial intelligence and optimization techniques, such as fuzzy, neural network, metaheuristic, etc.

Qi-Ye Zhang et al. (2014) have presented a clustering routing protocol based on type-2 fuzzy logic and ant colony optimization (CRT2FLACO) for WSN. In the process of clustering, a T2MFLS, a Type-2 Mamdnai fuzzy logic system, is used to manage the system overhead by determining the critical factors-residual energy, rate of neighbor nodes, and the division from the base station (BS) of a node.

F. Zhang et al. (2013) have proposed the ICT2TSK protocol, which combines the Old LEACH approach and the novel CHEATS protocol. These approaches are compared, and the development of two sides is more critical, namely Type-2 TSK FLS (Takagi-Sugeno-Kang Fuzzy Logic System) is developed to choose the CH by evaluating each node's option, which can handle the overhead higher than a type-1 TSK FLS. Guo et al. (2010) have developed a routing method based on the PEGASIS approach that is more beneficial than the Ant Colony Algorithm rather than the greedy algorithm to create the chain. The new PEG-ant global optimization is compared with the PEGASIS, which is good in the result.

J. M. Kim et al. (2008) have illustrated a novel CH selection in the wireless sensor network. It is based on the base station, which is dependable on designating CH within all rounds. All the network nodes can become cluster-head depending on concentration, energy, and centrality factors. Bouhafs et al. (2006) have developed a new clustering protocol based on semantic attributes for WSN. In the clustering process, the signal's energy of neighbor nodes is chosen as criteria, and nodes rank is evaluated within the cluster like a hypertree.

C. Li et al. (2005) have proposed the Energy Efficient Unequal Clustering (EEUC) methodology. This method detects the large-size clusters away from the BS, and then other clusters are smaller in size. In addition, the energy-aware multichip routing protocol is proposed for inter-cluster communication, which gives better results.M. Handy et al. (2002) have presented the expansion of a LEACH protocol used to mitigate the energy consumption of WSNs. This paper proposed a new strategy to improve the microsensor network's lifetime by implementing three new metrics,i.e., do not requires a BS for node communications, self-recognised to become CH, and due to this reason, communication energies are protected.

Kennedy et al. (1995) have presented a Particle Swarm Optimisation (PSO), which is motivated by the movement of a flock of birds or a school of fishes. The PSO is used to control the particle movement to perform optimization; the information of individual experience and socio-cognitive tendency are utilized. Cognitive learning and social learning are the user information, respectively, and direct the population to determine the best solution to perform optimization. Abbass et al. (2001) have proposed a Marriage in honey Bees Optimization (MBO) which is used to solve propositional satisfiability problems (3-SAT problems). In this algorithm, the queen bee mating flight is presented as the state space on transitions (search space), with the queen mating with the murmur encountered at every state. The queen's speed and energy and the drone's fitness are used to calculate the mating probability.

Karaboga et al. (2007) have presented an Artificial Bee Colony optimization (ABC), classified into three types: scout bees, employed bees, and onlooker bees. Therefore employed and onlooker bees are used for local search, and the scout bees are used for a global search for balancing exploration and exploitation

Krishnan et al. (2005) have presented a Glow-worm Swarm Optimization (GSO) [15], which belongs to the firefly behaviors. According to the luminescence and Firefly movement, it randomly chose a neighbor firefly. Using selective neighbor information, the behaviour of movement causes the firefly swarm o divide into disjoint subgroups to find multiple optima.

Yu et al. (2005) presented a new Social Spider Algorithm to solve global optimization issues. This method belongs to the spider's foraging strategy, which utilizes the spider web vibrations to find the prey's positions. In addition, developing guidelines are proposed for selecting the parameter values in the sensitivity analysis for this algorithm.

Jonathan et al. (2017) have proposed a FEAC-Stream, abbreviated as the Fast Evolutionary Algorithm for Clustering data streams. The Page–Hinkley Test is also used in FEAC-Stream to determine degradation in the induced cluster quality. Based on the assumption that clusters provide helpful information about the data stream dynamics. This algorithm is applied to data streams of synthetic and real-world.

Yongquan et al. (2017) have developed a simplex method-based social spider optimization (SMSSO) algorithm. This method is used to increase population diversity while developing the ability of local search spiders.

Chen et al. (2015) have illustrated a nodal belief evaluation of the clustering algorithm in a smart grid. For CH trust calculation, the data interactions between CH and intra-cluster nodes are considered, and finally, the number of interactions is set as a weight for trust calculation.

From the literature, no clustering algorithm considers the node's security and temperature rise. This work aimed to propose a clustering algorithm considering multiple clustering metrics.

4. Proposed Methodologies

In this section, the proposed methodology is classified into three stages. Initially, fuzzy clustering is done to form cluster nodes. Next, the important parameter of Trust degree Evaluation is presented for identifying the Trust degree of every individual node for security. Finally, the proposed Spider-Based Security and Energy Aware Clustering (SSEAC) are presented based on the Spider Optimization Algorithm (SOA) for enhancing Cluster Head selection by considering objective functions. Therefore the proposed SSEAC method workflow is presented with a corresponding algorithm and the formulations, which are explained in detail as follows.

4.1. Fuzzy-based clustering

The fuzzy-based clustering is the initial process proposed, which partitions an n-th number of objects as Y = y_1, y_2,..., y_n into a k-th number of fuzzy clusters C_1, C_2,...,C_k. The clustering state is indicated as n × k matrix M = [W_{ij}] which belongs between $1 \leq i \leq n$, $1 \leq j \leq k$. Where W_{ij} presents the belongingness degree of the i-th object to the j-th cluster. The matrix M = [wij] would satisfy the conditions given in the following(Mika Sato-Ilic *et al.*2014):

- For every y_i object and c_j cluster belongs to $0 \leq w_{ij} \leq 1$
- For y_i, $\sum_{j=1}^{k} w_{ij} = 1$
- For c_j, $0 \leq \sum_{j=1}^{k} w_{ij} < n$

On considering the above conditions, the matrix M = [W_{ij}] are satisfied where the W_{ij} is the belongingness degree that is expressed as:

$$W_{ij} = \frac{1/\mathrm{dist}(x_i,c_j)^2}{\sum_{l=1}^{k} 1/\mathrm{dist}(x_i,c_j)^2} \quad (1)$$

From the above Eq.1, c_j is the center cluster which belongs between $1 \leq j \leq k$. The dist(yi, cj) represents the distance between y_i and c_j, where x_i, is another object. According to Eq.3, the conditions of matrix M = [W_{ij}] are satisfied. Therefore, the fuzzy algorithm of initialization is illustrated in Algorithm1 in detail for cluster formation.

Algorithm 1: Fuzzy-based Cluster Formation

```
function Fuzzy cluster of (k,n)
for j=1 → k do
$C_j$ ← $y_{random(1,n)}$
end for
repeat
for i=1 → n do
    for j=1 → k do
    Apply $W_{ij}$ using Eq.1
    end for
end for
do until $C_j$ does not change j=1 → k
return W
end for
end function
```

According to the above algorithm, cluster formation can be done with the optimum results on grouping. The next process is to apply every node to a cluster based on its belongingness degree before each round. Therefore object y_i is applied to C_j when it satisfies Equation 2.

$$\sum_{l_1=1}^{j-1} w_{il_1} \leq r < \sum_{l_2=1}^{j} w_{il_2} \tag{2}$$

Where r is a random number between 0 and 1. After that, the Spider Optimization Algorithm is applied to select CH based on the Trust degree and Objective function in the Smart wireless grid.

4.2 Trust Degree Evaluation

In this section, efficient analysis of the trustworthiness of each node can be evaluated for the Cluster Head selection, which is focused on both trust degree and quality for maintaining the QoS of the smart grid. Many attacks have occurred in the mesh network, which is mentioned in section II that attacks are increased the eavesdropping job. The eavesdroppers reduce the network quality where the trust degree of the node is decreased, and the malicious nodes will access the cluster heads. Therefore the wireless sensor networks required an efficient methodology to overcome these issues where the Trust Degree Evaluation approach is presented. This approach is used to enhance the security of every node and to select the CH easily with a high Qos of Smart grid.

The parameter of trust degree evaluation is an analysis that can be used to maintain the basic decision of the nodes in the system. This calculation is used to help the sensor nodes from the parent network to manage vulnerability about the future actions of another neighbor node.

Initially, entire nodes in the mesh network are permitted to transfer the data packets during the network formation. When the packets are transferred from one node to another, the energy and the number of successful and unsuccessful nodes are measured. The nodes that can be processed within the predetermined time period are analysed as successful nodes. The nodes with the delayed outcome in data transmission will be noted as unsuccessful data transmission nodes. On analysis of the number of successful and failed transmissions, the trust degree of each node is computed. The CH can be easily optimised with high-energy nodes with good trustiness.

According to this evaluation, the node-to-node trust degrees are computed by the cluster's number of successes and failures in data transmission. All the trust degree of cluster nodes in the networks is updated with the routing table and the neighbour node inside the cluster. Therefore, this calculation consumes less computation time which can easily satisfy the QoS and QoE requirements.

The Trust Degree Evaluation of every individual node in the cluster is expressed in Eq.(3)

$$T_{x,y} = \left|\left(\left[10.\ S_{x,y}(\Delta t)\right] / \ S_{x,y}(\Delta t) + U_{x,y}(\Delta t)\right) \left(\frac{1}{\sqrt{U_{x,y}}}\right)\right| \tag{3}$$

Where Δt represents the time window, $S_{x,y}$ is the positive data transmission and $U_{x,y}$indicates the failure of data transmission respectively.

If the attacker node has a high trust degree which can eavesdrop on the packet transmission through the black hole node and sink hole, the malicious nodes drop the data packets. Therefore from the above equation, the trust degree of each node can be easily computed for the positive and failure data transmission, which enhances the QoS effectively.

4.3 Design of Fitness Function

The Fitness function is an important topology that can be controlled to minimize the total energy consumption during node communications. This paper shows that the distance between every member node can affect energy consumption. Therefore, in this paper, some of the important factors taken to compute the objective functions are given in the following.

4.3.1 Average distance between each node to CH

The overall system is partitioned into a K-number of clusters in the group with $N_{i,}$ a node inside the cluster. Therefore, the maximum average distance is expressed in Eq. (4)

$$dist_{mem-CH} = i = 1,2,\dots,K^{max}\left\{\frac{\sum_{j=1}^{N_i}(CM_{ij},CH_{ij})}{N_i}\right\} \tag{4}$$

Where i = 1, 2,…, K, and K denotes the number of nodes in CH

CH nodes to the BS based Maximum average distance is expressed as:

$$dist_{CH-BS} = i = 1,2,\dots,K^{max}\{d(CH_i,BS)\} \tag{5}$$

4.3.2 Energy consumption of an overall network

The total energy consumption of the network is given in the following Eq.(6)

$$E_{tot} = \sum_{i=1}^{K}\left(E_{CH}^{i} + \sum_{j=1}^{N_i}\left(E_{mem}^{ij}\right)\right) \quad (6)$$

Where $\boldsymbol{E_{CH}^{i}}$ indicates the CH's energy consumption i during a round and $\boldsymbol{E_{mem}^{ij}}$ presents the node's energy consumption in cluster i during a round.

4.3.3. RSS for power consumption

In the WSN, the power utilization is limited resources and very low power storage for data transmission. This limited power leads to a signal for weak communication with the base station. The receiver signal strength (RSS) is computed during wireless communication to overcome these issues. When the node has less RSS value, then the node cannot send packets properly to BS or use more power for data transmission.

The RSS is used to find the cluster size where the node's energy consumption is reduced by the transmission distance between the node and the CH. In the equation, the average RSS between these nodes (RSS_{nodes}) expressed in the following.

$$RSS_{nodes} = \frac{\sum_{i=1}^{N_c} RSS(i)}{N_c.RSS_{max}(i)} \quad (7)$$

Where $RSS(i),$ the RSS is the value of the i-th node and also RSS_{max} represents the maximum RSS of the i-th neighbor. N_c is the overall current neighbour's values.

On considering the important parameters for the secured CH selection, the fitness value of the objective function is expressed in the below Eq.(8).

$$\mathrm{F} = \alpha \mathrm{dist}_{\mathrm{mem-CH}} + \beta \mathrm{dist}_{\mathrm{CH-BS}} + \gamma \mathrm{E}_{\mathrm{tot}} + \sigma \mathrm{RSS}_{\mathrm{nodes}} + \delta \mathrm{T}_{\mathrm{x,y}} \quad (8)$$

According to the above equation, It is normalized to the maximum average values for the secured and energy overhead network. The parameters α, β, γ,σ and δ are used to determine the weight priority distance from the member node to CH, the total energy consumption of the network, CH to BS's maximum distance, the RSS of every member node, and the trust degree of each node with of α+β+γ+σ+δ=1 respectively.

4.4 Proposed SSEAC Algorithm

4.4.1 Problem statement

The CH node's security and energy consumption are the main troubles in the wireless smart grid. Therefore, a cautious and trust degree consideration is required for each node before selecting CHs. In the proposed SSEAC method, initially, Fuzzy is used for clustering the nodes, and then the SOA is performed and applied with an objective function for an efficient CH selection. Therefore, the SOA must evaluate a fitness function by updating distances, energy consumption, and Trust degree of nodes for the best CH selection. The fuzzy clustering and SOA are combined to present an SSEAC method explained in Algorithm 2.

4.4.2 Spider Optimization Algorithm (SOA)

The spider Optimization Algorithm (SOA) is based on the Swarm Intelligence Algorithm, which is proposed by analysis the behaviours of spiders. This optimization algorithm's main agent is the spider used for the cluster Head selection. The SOA algorithm is initiated with the analysis of the spider's population, which is located on the web. The basic behaviour of each spider is holding memory and also storing every piece of information mentioned as follows:

- Spider's position on the web.
- The present position fitness of spider
- In the existing iterative process, the spider's vibration is targeted.
- When the Spider has changed its target vibration, then the number of iterations from the time is measured
- Note the progress of the spider that is performed in the previous iteration.
- The Spider is employed to direct movements in the previous iteration using a dimension mask

In the SOA algorithm, the initialization step is carried out for locating spiders. Next, the search progress is performed iteratively. At last, the algorithm is terminated if the required outcomes of optimal solutions are calculated. The main step of the SOA algorithm is calculating the fitness values for every individual artificial spider with its various locations. Then, the SOA updates the optimum global value, if possible. During every iterative progress, each spider's fitness values are calculated. After that, entire spiders will make a vibration at their positions using Eq.(9).

$$I\left(p_{spy}, p_{spy,t}\right) = \log\left(\frac{1}{f\left(p_{spy}\right) - C}\right) + 1 \quad (9)$$

Where $I\left(p_{spy}, p_{spy,t}\right)$ represents the spider's vibration rate produced in the position at time t. 'spy' indicates a spider. Pspy t represents the spider's position at time t. f(Pspy) indicates the fitness value of the spider in its present position. C represents the confidently less constant where all fitness values are larger than the C value for minimization issues. Logarithmic operations are done with the numbers are too large or too small.

Calculating an attenuation of vibration using the vibration generated by the spider in the source location and distance are two main properties shown in Eq.(10).

$$I\left(p_{spy1}, p_{spy2,t}\right) = I\left(p_{spy}, p_{spy,t}\right).exp\left(-\frac{D\left(p_{spy1}, p_{spy2}\right)}{\bar{\sigma}.r_a}\right) \quad (10)$$

Where $D\left(p_{spy1}, p_{spy2}\right)$ represents the distance between spider1 and spider2 (i.e.). The distance is calculated by Eq.(11)

$$D\left(p_{spy1}, p_{spy2}\right) = p_{spy1} - p_{spy2} \quad (11)$$

According to Eq.(11), the spider's vibrations are used to activate the process of propagation (Yu and Li 2015).

Consider 'Vb' as the vibration of spiders, whereas every spider receives another spider's vibrations. On getting the vibration, the spider used to choose the best and most robust vibration rate of spider which is termed as 'Vb_{spy}^{best}'. The vibration received spider is used to store the target vibration, which is indicated as 'Vb_{spy}^{target}'. Then every individual Spider was used to compare the values of Vb_{spy}^{best} and Vb_{spy}^{target}. If the Vb_{spy}^{best} intensity is greater than Vb_{spy}^{target}, then the Vb_{spy}^{target} is changed to as Vb_{spy}^{best}. Then the random walk of every spider is calculated using the following Eq. (12)

$$P_{spy}(t+1) = P_{spy} + \left(P_{spy} - P_{spy}(t-1)\right).r + \left(P_{spy}^{follow} - P_{spy}\right) \odot R \qquad (12)$$

Where R represents the random vector of float point from zero to one uniformly. ⦿ Indicates an element-wise multiplication. 'P_{spy}^{follow}' is the following position where every spider looks at the dimension mask to decide theP_{spy}^{follow}.

After the dimension mask (DM) calculation, a new following position is generated using the dimension mask. A new following position of $P_{spy,i}^{follow}$ is calculated by Eq. (13)

$$P_{spy,i}^{follow} = \begin{cases} P_{spy,i}^{target} & DM_{spy,i}=0 \\ P_{spy,i}^{r}, & DM_{spy,i}=1 \end{cases} \qquad (13)$$

Where 'r' represents the random integer value and $DM_{spy,i}$ stands for the ith dimension of the dimension mask of the spider.

```
Algorithm2: PROPOSED SSEAC Algorithm
Step 1: Initialize the Random source position of the
        spider and assign the Target Vibration of each
        Spider in memory.
Step 2: Evaluate the Fitness Value of each Spider and
        find the best solution using Eq.
Step 3: Calculate the Vibration values of every spider
        using Eq.(9,10&11)
Step 4: Compare the values of the Best Vibration and
        Target Vibration of every Spider
Step 5: Determine the Dimension Mask
Step 6: Calculate the Following Position of the Spider
        using Eq.(13)
Step 7: Update the movement of each spider using Eq.
        (12)
Step 8: Repeat the process from step 3 until the results
        obtained
Step 9: Output of optimum results are obtained
```

5. Experimental Results

To validate the proposed cluster head selection approach MATLAB tool has been used. Table 1 presents the simulation parameters of this work. For simulation, a similar model of Priya et al. (2020) is used as an energy model.

To validate the proposed technique's efficiency, parameters like the number of nodes alive and the total data message successfully received are compared with conventional LEACH, Fuzzy Clustering PSO (FCPSO), and fuzzy clustering SSO (FCSSO) techniques. As shown in Figure 1, the proposed clustering effectively chooses CH and transfers more messages than other methods. Considering CH selection, all the factors can ensure that more data is delivered to BS.

Table 1. Simulation parameters

Parameter	Value
Number of nodes	100
Distributed area	500*500
Initial energy of sensor node (Ei)	2J
Packet length(l)	4000 bit
α-factors	0.2
β-factors	0.2
γ-factors	0.2
σ-factors	0.2
□-factors	0.2

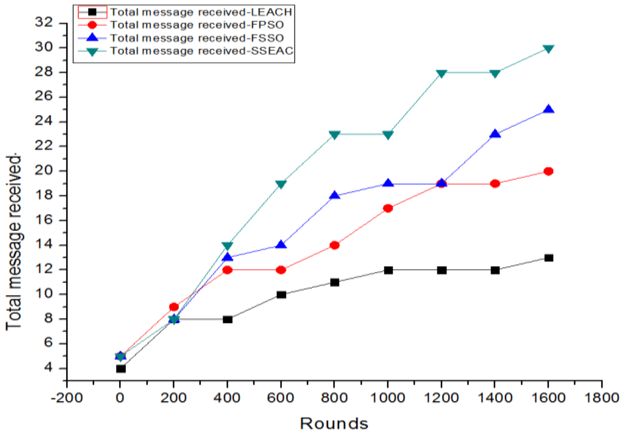

Fig. 1 Total number of the message received by the base station versus rounds

Fig.2 observed that the proposed SSEAC increases the number of the living node by selecting proper CH considering the distance to other member nodes. Compared to FSSO, SSEAC shows less number of living nodes due to the additional overhead of security-related packet transfer.

The simulation has been performed for the various selective forwarding attacks, data forgery attacks, on-off attacks, conflicting behavior attacks, and data tampering attacks. The attacker percentage varies from 5 to 25 percent. As shown in Figure 3, the proposed trust degree approach gives a higher detection rate. Hence, the proposed clustering is an efficient trust evaluation model that can categorize different malicious nodes and can be dynamically adapted according to the network's specific requirements.

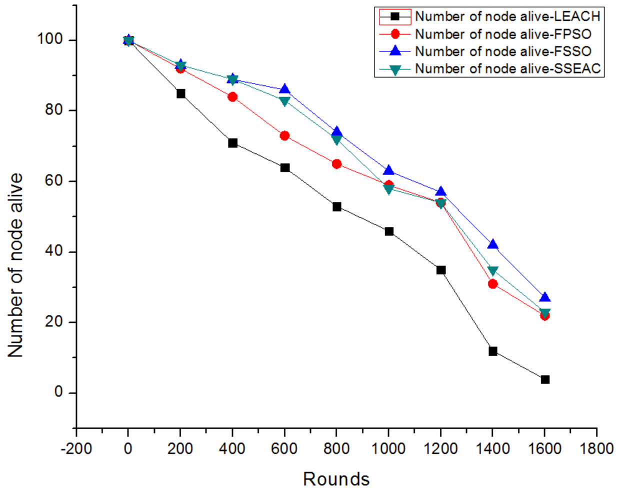

Fig. 2 Total number of nodes alive vs. rounds

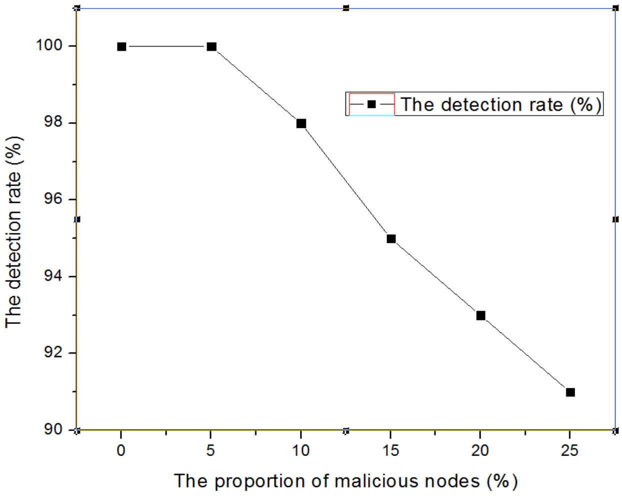

Fig. 3 Shows the detection rate versus the proportion of malicious nodes (%)

The average message delivery rate to a base station is calculated for varying attacker percentages, as shown in figure 4. The proposed algorithm produces an assured level delivery rate due to the detection and avoidance of the attacker Detection Rate attackers participating in the clustering process. The other methods show less delivery rate for a higher proportion of malicious nodes due to the participation of forgery and selfish nodes.

In LEACH, the overall clustering efficiency reached up to 89%. It accounts for distance as a clustering metric. In FPSO, the distance, energy, and distance to the sink node are considered clustering metrics .It reaches a

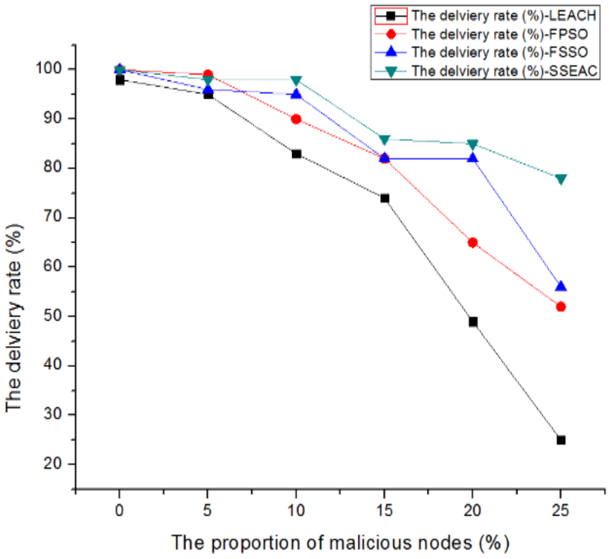

Fig. 4 The delivery rate (%) versus the proportion of malicious nodes (%)

clustering efficiency of 93.6%. But, failed to work when the presence of attackers. The proposed SSEAC achieves the overall clustering efficiency of 97.3% even in the presence of malicious nodes in the network due to the consideration of trust degree as a clustering metric.

6. Conclusion

This paper proposes Spider-Based Security and Energy Aware Clustering (SSEAC) for Wireless Smart Grid Networks. This proposed system can be used to enhance both the security and the energy overhead by selecting an efficient cluster head for wireless data transmission. This SSEAC can be processed the security based on the trust degree of each node for the improvement of QoS in the smart grid. This method considers the main factors of the distance between a node to CH, the distance between CH and BS, total energy consumption, RSS of each node, and the Trust degree evaluation of each node in the cluster which is processed with the SOA to generate an optimal result for CH selection. Therefore, the results of SSEAC clearly show that the entire network of the wireless smart grid is more secure than the conventional methodologies. On focusing on the security of nodes for data transfer, a trust degree-based evaluation is a good attempt to take over the attacks presented in the network. However, the proposed SSEAC method is much better in the result of accuracy. Also, it improves the lifetime of networks with high security and less energy consumption with a high packet delivery ratio than the previous methods.

References

[1] Qi-Ye Zhang, Ze-Ming Sun and Feng Zhang, "A Clustering Routing Protocol for Wireless Sensor Networks Based on Type-2 Fuzzy Logic and ACO", *2014 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, July 6-11, 2014, Beijing, China.

[2] C Sunil Kumar, Puttamadappa C, Y L Chandrashekar, "Bacterial Foraging and Seagull Optimization Algorithm Based THD Level Comparison for Flyback Converter in Grid-Connected PV System," *International Journal of Engineering Trends and Technology*, vol. 70, no. 6, pp. 379-394, 2022. Crossref, https://doi.org/10.14445/22315381/IJETT-V70I6P238.

[3] H. Khurana, Et Ai., "Smart-Grid Security Issues," *Security & Privacy, IEEE*, vol. 8, pp. 81-85, 2010.

[4] F. Zhang, Q. Y. Zhang, Z. M. Sun," ICT2TSK: An Improved Clustering Algorithm for WSN Using a Type-2 Takagisugeno-Kang Fuzzy Logic System, *2013 IEEE Symposium on Wireless Technology and Applications (ISWTA),* September 22-25, Kuching, Malaysia, pp. 153-158, 2013.

[5] W. Guo, W. Zhang, G. Lu," PEGASIS Protocol in Wireless Sensor Network Based on Improved Ant Colony Algorithm," *2010 Second International Workshop on Education Technology and Computer Science, Wuhan: IEEE Computer Society*, pp. 64-67, 2010.

[6] J. M. Kim, S. H. Park, Y. J. Han, and T. M. Chung," CHEF: Cluster Head Election Mechanism Using Fuzzy Logic In Wireless Sensor Networks," *In Proceedings of the International Conference on Advanced Communication Technology (ICACT),* pp. 654-659, 2008.

[7] D.Bharathy Priya, Dr.A.Sumathi, Dr.J.Karthikeyan, "Integrating Renewable Energy System in Smart Grid Applications," *SSRG International Journal of Electronics and Communication Engineering*, vol. 6, no.6, pp.1-4, 2019. *Crossref,* https://doi.org/10.14445/23488549/IJECE-V6I6P101.

[8] F.Bouhafs, M. Merabti, and H. Mokhtar, "A Semantic Clustering Routing Protocol for Wireless Sensor Networks," *IEEE Communications Society Subject Matter Experts for Publication In the IEEE CCNC 2006 Proceeding*s.

[9] C. Li, M. Ye, G. Chen, and J. Wu," An Energy-Efficient Unequal Clustering Mechanism for Wireless Sensor Networks," *In IEEE International Conference on Mobile Adhoc and Sensor Systems Conference (MAHSS),* pp. 597-604, 2005.

[10] M. Handy, M. Haase, D. Timmermann," Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection," *In the 4th International Workshop on Mobile and Wireless Communications Network*, Citeseer, pp. 368- 372, 2002.

[11] J. Kennedy, R. Eberhart, “Particle Swarm Optimization,” *In: Proceedings of ICNN'95 - International Conference on Neural Networks,* Perth, WA, US, pp. 1942–1948, 1995.

[12] H. A. Abbass, “MBO: Marriage in Honey Bees Optimization-a Haplometrosis Polygynous Swarming Approach,” *In: Proceedings IEEE Congress on Evolutionary Computation (CEC),* Seoul, Korea, pp. 207–214, 2001.

[13] P.Ramya, "Load Distribution of SPR and CSR In Wireless Network," *International Journal of Recent Engineering Science (IJRES)*, vol. 1, pp. 16-21, 2014.

[14] D. Karaboga, B. Basturk, “A Powerful and Efficient Algorithm for Numerical Function Optimization: Artificial Bee Colony, ” *The Journal of Global Optimization*, vol. 39, no. 3, pp. 459–471, 2007.

[15] K. Krishnanand, D. Ghose, “Detection of Multiple Source Locations Using a Glowworm Metaphor with Applications to Collective Robotics,*” In: Proceedings IEEE Swarm Intelligence Symposium*., Pasadena, CA, US, pp. 84–91, 2005.

[16] Priya, R. K., & Venkatanarayanan, S, “ Implementation of Thermal Aware Wireless Sensor Network Clustering Algorithm Based on Fuzzy and Spider-Optimized Cluster Head Selection, ” *Journal of Ambient Intelligence and Humanized Computing*, 2020.

[17] Nishant Jakhar, Rainu Nandal, Kamaldeep, "Design of A Rule-Based Decisive Model for Optimizing the Load Balancing in a Smart Grid Environment," *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp. 97-103, 2022. Crossref, https://doi.org/10.14445/22315381/IJETT-V70I8P209.

[18] Yu, J. J. Q., & Li, V. O. K, “ A Social Spider Algorithm for Global Optimization, ” *Applied Soft Computing*, vol. 30, pp. 614–627, 2015. Doi:10.1016/J.Asoc.2015.02.014.

[19] Jonathan De Andrade Silva, Eduardo Raul Hruschka, João Gama," An Evolutionary Algorithm for Clustering Data Streams with a Variable Number of Clusters," *Expert Systems with Applications*, vol. 67, pp. 228-238 , 2017.

[20] Yongquan Zhou, Yuxiang Zhou, Qifang Luo, Mohamed Abdel-Basset, "A Simplex Method-Based Social Spider Optimization Algorithm for Clustering Analysis," *Engineering Applications of Artificial Intelligence*, vol. 64, pp. 67-82, 2017.

[21] Chen, C., Xiaomin Liu, Hualin Qi, Liqiang Zhao, & Zhiyuan Ren, “A Security Enhancement and Energy Saving Clustering Scheme in Smart Grid Sensor Network,” *2015 IEEE 16th International Conference on Communication Technology (ICCT),* 2015. Doi:10.1109/Icct.2015.7399960 .

[22] Mika Sato-Ilic, “Universal Fuzzy Clustering Model,” *In Proceedings of the IEEE International Conference on Fuzzy Systems (IEEE-FUZZ), IEEE,* pp. 2071–2078, 2014.