f

Trust Aware Moth Flame Optimization based Secure Clustering for Wireless Sensor Networks

Abdul Rahaman Wahab Sait[1], M. Ilayaraja [1]

[1] King Faisal University, Kingdom of Saudi Arabia

[2] Department of Computer Science and Information Technology, Kalasalingam Academy of Research and Education, Krishnankoil, India

Emails: asait@kfu.edu.sa ; ilayaraja.m@klu.ac.in

Abstract

Wireless sensor networks (WSN) encompass numerous sensor nodes deployed in the physical environment to sense parameters and transmit to the base station (BS). Since the nodes in WSN communicate via a wireless channel, security remains a significant issue that needs to be resolved. The choice of cluster heads (CHs) is critical to achieving secure data transmission in WSN. In this aspect, this article presents a novel trust-aware mothflame optimization-based secure clustering (TAMFO-SC) technique for WSN. The goal of the TAMFO-SC technique is to determine the trust level of the nodes and determine the secure CHs. The proposed TAMFO-SC technique initially determines the nodes' trust level, and the node with maximum trust factor can be chosen as CHs. In addition, the TAMFO-SC technique derives a fitness function using two parameters, namely residual energy and trust level. The inclusion of trust level in the CH selection process helps to accomplish security in WSN. A comprehensive experimental analysis exhibits the promising performance of the TAMFO-SC technique over the other compared methods.

Keywords: Wireless sensor networks, Trust level, Security, Clustering, Cluster heads, Moth flame optimization, Energy efficiency.

1. Introduction

With the rapid growth of sensing technology, wireless communications, and electronics, wireless sensor networks (WSN) [1] has gained huge interest. WSN includes several WSNs that contains data processing, short distance sensing, and wireless communication function. This embedded sensor works together and is self-organizing to collect and sense each kind of stimulating environmental information. Furthermore, the process and analyze the novel information for obtaining precise data in many environment scenarios [2]. The outstanding features of WSN make it possess extensive application prospects in environmental monitoring, military defense, medical, biological, commercial applications, disaster relief, etc. [3]. Generally, the WSNs node is armed with a separate battery and typically positioned of huge numbers in remote locations that people nearly couldn't attain. It is a complex process for recharging/replacing the sensor's battery. To decrease the power utilization, the transmission range of the nodes is severely restricted. The topology protocol of WSNs generally emphasis how to split the entire networks to cluster and create multihop constructions amongst these CHs to transfer sensory information to BS through self-organization. In dynamic, open, and distributed environments, the building of network topology, is susceptible, resulting in whole networks being dangerous. Fig. 1 illustrates the structure of WSN. For the WSN method, guaranteeing the privacy of the transmission is a significant problem in building network topologies [4].

DOI: https://doi.org/10.54216/JISIoT.050202

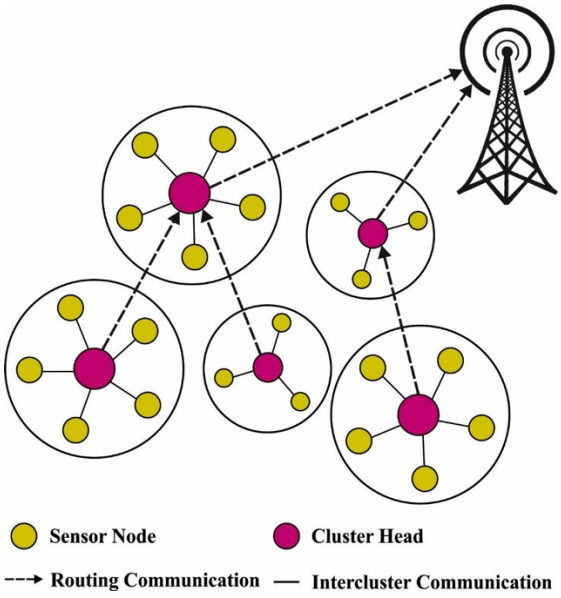

Fig. 1. WSN structure

Recently, a person has progressed to distinct privacy routing protocols. Many of this is on the conventional privacy mechanism of the cryptosystem that requires additional energy and memory utilization [5]. The WSN comprises multiple smaller sensors with constrained stringent and bandwidth nodes based on memory and power. The cryptosystem could withstand external attacks; they won't be recognized once the internal node has attacks/mutations. Hence the conventional cryptosystem of the privacy methodology isn't completely related to WSNs [6]. To resolve the challenges mentioned above, the authors have presented the trust management method. Trust is determined by the binary relationship arising in object and subject. Several CH algorithm was presented for WSNs [7]. Many of this CH method focuses on energy-effective CH election. The privacy aspects of CH node aren't taken into account while developing CH election method [8]. Hence, this algorithm must be developed to securely select CH via observing the bargained hubs and rejecting them of their CH candidacy in WSNs.

This article presents a novel trust aware mothflame optimization-based secure clustering (TAMFO-SC) technique for WSN. The goal of the TAMFO-SC technique is to determine the trust level of the nodes and determine the secure CHs. The proposed TAMFO-SC technique initially determines the nodes' trust level, and the node with maximum trust factor can be chosen as CHs. In addition, the TAMFO-SC technique derives a fitness function using two parameters: residual energy (RE) and trust level. The inclusion of trust level in the CH selection process helps to accomplish security in WSN. A comprehensive experimental analysis exhibits the promising performance of the TAMFO-SC technique over the other compared methods.

2. Related works

In Miglani et al. [9], an EETA-LEACH was presented, enhancing LEACH protocol by presenting trust to offer secure routing when preserving the novelty of LEACH protocols. These approaches integrate trust-based routing model and trust management model, which collaborates for selecting trusted CH. Gaber et al. [10] present a bioinspired and trust-based CH method for WSN adapted in ITS application. A trust-based method is developed and utilized for computing a trust level for all nodes. The BOA is utilized for selecting the CHs according to 3 variables: numbers of neighbors, RE, and trust value.

Karthick [11] developed a new method for the secured routing of WSN. The presented model is called TDP. According to the presented method, the routing is made in 4 phases. The early phase is topology management with the k-means model. The next phase is LQA, whereas the quality of all the network nodes is estimated. The last phase is grading, where it depends on the LQA values, and a grade point is selected for each node in the network. The more secured path for the routing is defined according to the grade point in the last stage. Yang et al. [12] developed a game theory-based dynamic behavior monitoring system for evidence collection

DOI: https://doi.org/10.54216/JISIoT.050202

in WSN. A tradeoff between energy conservation and network security is attained. According to this behavior monitoring system, a trust calculation method has been presented that is additionally incorporated with cluster-based routing protocols.

Sun and Li [13] proposed a new TRPM for WSN that integrates multi-attributes of sensors based on data, communication, recommendation, and energy. The presented trust method is based on an enhanced sliding time windows taking into account the frequency of the attacks for facilitating the detection of malicious behavior of the hackers. Integrated to an efficient maintenance protocol and routing detection, the performance of this result is verified by a wider range of simulations. AlFarraj et al. [14] presented an AF-TNS for resource-limited WSN for enhancing network safety. AF-TNS functions in 2 stages: trust assessment with energy limitation and preservative metric-based node assessment for retaining the reliability of the neighbor. The arbitrary Transigmoid functions simplify the complicated decision-making procedure of the AF through differentiating un-trusted and trusted nodes for controlling network performances.

3. The Proposed Model

The nocturnal performance of moths is the stimulation to MFO is presented in 2017. In this model, the exploration and exploitation balance consider a partition of candidate solutions generating the population:

- Pathfinder (for exploring novel regions of search space).
- Prospector (for exploiting the novel area get by the pathfinder).
- Onlooker (for analyzing the optimal area found by the prospector).

With another Metaheuristics, this one start with initiating a population:

$$x_{ij} = rand \cdot \left(u_j - l_j\right) + l_j, \forall i \in \{1, 2, n\}, j \in \{1, 2, d\} \tag{1}$$

Here, u & l represent the upper limit and lower limit of the search space, x_i indicates the candidate solution, n denotes the population size, d signifies the dimension problem, and *rand* indicates an arbitrary number derived from a standard distribution [15].

To make the pathfinder cross-over it is essential to compute the variation coefficient and dispersal degree at iteration t:

$$\sigma_j^t = \frac{\sqrt{\frac{1}{n_p}\sum_{i=1}^{n_p}\left(x_{ij}^t - P_j^t\right)^2}}{P_j^t} \tag{2}$$

$$\mu^t = \frac{1}{d}\sum_{j=1}^{d}\sigma_j^t \tag{3}$$

Whereas n_p represents the number of pathfinders, and

$$P_j^t = \frac{1}{n_p}\sum_{i=1}^{n_p} x_{ij}^t \tag{4}$$

In MFO, the crossover point with the low dispersal value, based on:

$$j \in c_p \; if \; \sigma_j^t \leqslant \mu^t \tag{5}$$

From those, only $n_c \in c_p$ crossover point is being utilized to generate a novel sub-trial pathfinder vector $\rightarrow \overrightarrow{v_p} = \left[v_{p1}, v_{p2}, \ldots, v_{pn_c}\right]$ from the original pathfinder $\overrightarrow{x_p} = \left[x_{p1}, x_{p2}, \ldots, x_{pn_c}\right]$ by:

$$\overrightarrow{v_p^t} = \overrightarrow{x_{r^1}^t} + L_{p1}^t \cdot \left(\overrightarrow{x_{r^2}^t} - \overrightarrow{x_{r^3}^t}\right) + L_{p2}^t \cdot \left(\overrightarrow{x_{r^4}^t} - \overrightarrow{x_{r^5}^t}\right) \tag{6}$$

$$\forall r^1 \neq r^2 \neq r^3 \neq r^4 \neq r^5 \neq p \in \left\{1, 2, \ldots, n_p\right\}$$

DOI: https://doi.org/10.54216/JISIoT.050202

Whereas L_{p1} & L_{p2} represent independent variables calculated from Lévy α-stable distribution. The group of indexes r should be chosen in the pathfinder solution, and this position is upgraded by the mutated variable extracted from the sub-trail vectors as follows:

$$V_{pj}^{t} = \begin{cases} v_{pj}^{r} \text{ if } j \in c_p \\ x_{pj}^{t} \text{ if } j \notin c_p \end{cases} \tag{7}$$

Lastly, MFO employs selection strategies among the original and trial pathfinders determined by:

$$\overrightarrow{x_p^{t+1}} = \begin{cases} \overrightarrow{x_p^t} \text{ if } f\left(\overrightarrow{V_p^t}\right) \geq f\left(\overrightarrow{x_p^t}\right) \\ \overrightarrow{v_p^t} \text{ otherwise} \end{cases} \tag{8}$$

The likelihood of selecting the succeeding pathfinders are determined by:

$$p_p = \frac{fit_p}{\sum_{p=1}^{n_p} fit_p} \tag{9}$$

That use the luminescence intensity evaluated as follows:

$$fit_p = \begin{cases} \dfrac{1}{1+f_p} & if\ f_p \geq 0 \\ 1 + |f_p| & otherwise \end{cases} \tag{10}$$

From the pathfinder, n_f individual is chosen as a prospector; this value is dynamically changed as:

$$n_f = round\left(\left(n - n_p\right) \times \left(1 - \frac{t}{T}\right)\right) \tag{11}$$

With T presence, the maximal iteration number. For simulating a prospector moth moving from the spiral manner over pathfinders (as in natural counterpart), MFO use the succeeding determination:

$$x_i^{t+1} = \left|x_i^t - x_p^t\right| \cdot e^{\theta} \cdot cos2\pi\theta + x_p^t \tag{12}$$

$$\forall p \in \{1, 2, \dots, n_p\}; i \in \{n_p + 1, n_p + 2, \dots, n_f\}$$

In which $\theta \in [r, 1]$ represent an arbitrary value used for giving a spiral shape to the prospector path, where $r = -1 - t/T$.

The onlooker is the moth with the minimum luminescent intensity that moves to the shiniest source of light; in MFO, the onlooker stage has been used to intensify the exploitation of promissory spot the search spaces. The onlooker groups are additionally separated into two movement rules: Gaussian walks and associative learning mechanisms with immediate memory. Firstly, the onlooker in the actual iteration has been attained as follows:

$$x_i^{t+1} = x_i^t + \varepsilon_1 + \left[\varepsilon_2 \cdot best_g^t - \varepsilon_3 \cdot x_i^t\right], \forall i \in \{1, 2, \dots, n_o\} \tag{13}$$

Whereas ε_2 & ε_3 are uniformly distributed arbitrary numbers, $best_g$ denotes the global optimal candidate solution, $n_o = round(n_u/2)$ indicates the number of onlookers which perform a Gaussian motion, n_u represents the number of onlookers, and ε_1 means an arbitrary value evaluated by

$$\varepsilon_1 \sim random\big(size(d)\big) \oplus N\left(best_g^t, \frac{logt}{t} \cdot \left(x_i^t - best_g^t\right)\right) \tag{14}$$

The behavior of the moth considers associative learning and short term memory, upgrade as:

$$x_i^{t+1} = x_i^t + 0.001 \cdot G + \left(1 - \frac{g}{G}\right) \cdot \varepsilon_2 \cdot \left(best_p^t - x_i^t\right) +$$

DOI: https://doi.org/10.54216/JISIoT.050202

$$\left(\frac{2g}{G}\right)\varepsilon_3 \cdot \left(best_p^t - x_i^t\right), \forall i \in \{1, 2, n_m\} \quad (15)$$

With $n_m = n_u - n_o$ being the number of onlookers who perform short-term memory and associative learning, $1 - g/G$ denotes a cognitive factor, $2g/G$ indicates a social factor, $best_p$ represents the optimal light source in the pathfinder's group and $G \sim N\left(x_i^t - x_i^{min}, x_i^{max} - x_i^t\right)$. The MFO pseudo-code shows each step of the original technique was illustrated in Algorithm 1.

Algorithm 1: Moth Swarm Algorithm pseudo-code

Initiate the population

Evaluate fitness of the swarm; sort population based on its fitness; chose n_p

The moth is a pathfinder; find onlookers and prospectors.

while $t < T$

pathfinder stage

prospector stage

onlooker stage

find novel light sources and types of every moth

end while

print global optimal

Let WSN of n sensors have been utilized arbitrarily. For CH selective, the projected OAFS applies a fish population used to generate suitable clusters and maintain the minimum power consumption of the model. Let $X = (X_1, X_2, \ldots, X_n)$ represent the population vector of WSN with n sensor, where $X_i(j) \in \{0, 1\}$. The CH and normal nodes have been demonstrated as 1 and 0. The whole population of NP solutions is stimulated arbitrarily with implies of 0s and 1s and shown as:

$$X_i(j) = \begin{cases} 1, & if\left(rand \leq p_{opt}\right) \\ 0, & otherwise \end{cases} \quad (16)$$

Where p_{opt} signifies the recommended percentage of CHs, and *rand* refers to the arbitrary uniform value in 0 and 1. An arbitrarily placed sensor nodes are decided that K clusters: $\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_\mathrm{K}$. The CH election has been responsible for decreasing the cost of FF. Therefore, the FF to CH election is illustrated as:

$$f_{\mathrm{obj\_CH}} = \sum_{\mathrm{i=1}}^{2} w_i \times f_i \quad (17)$$

with: $\sum_{i=1}^{2} w_i = 1$. Maximal stability period has been able with decreasing the Standard Deviation (SD) of RE of node is the main concern. Therefore, the SD (σ_{RE}) has been appropriate to measure the supremacy of uniformly distributed load in sensors. In addition, the trust level is considered as another factor for CH selection.

A security-based trust is mainly based on the trust computations of a provided node. In general, there are 2 phases to calculate and manage the reliability of the node in the presented result: BS level and node level (CH node and average node).

In the Trust on Node Level phase, all the nodes are accountable for monitoring their neighbor's behaviors and calculating their trust value according to certain matrices. All the trust matrices have a specific weight that provides the capacity for controlling or adjusting the priority of all the matrices based on the essential applications. Eq. (18) represents how straightforward trust values are estimated as node i for node j.

DOI: https://doi.org/10.54216/JISIoT.050202

$$DT(i,j) = \sum_{k=1}^{m} W_k * T_k(i,j) \quad (18)$$

In the equation, m represents the number of trust matrices; W_k indicates the weight values of the k metric thus $\sum_{k=1}^{m} W_k = 1$; $T_k(i,j)$ represents the trust values fixed as node i on k metric for node j. CH calculates the reliability of the node in its cluster by Eq. (18); next, ask all the members in its cluster to send the value we calculated regarding their neighbor in the similar clusters. With Eq. (19), CH computes the aggregated trust values of all the nodes. Next, it gets the overall trust values of the node in its cluster by

$$AT(j) = \frac{1}{h} * \sum_{r=1}^{h} D\,T(r,j) \quad (19)$$

Whereas h represents the amount of neighboring nodes j; $DT(r,j)$ represents the straightforward trust values calculated using node r for node j.

$$TT(j) = W_a * DT(CH,j) + W_b * AT(j) \quad (20)$$

In which W_a & W_b represent weighting aspects, thus $W_a + W_b = 1$.

At the trust on BS phase, the node transmits the estimated value to the adjacent BS to aggregate them and detect the last trust value Later, it estimates that node is trusted and malicious with a user-determined threshold. Eq. (19) represents the aggregated values are calculated for j node. Also, Each BS collects trust value aggregated with another BS to be utilized as an indirect trust observation. Additionally, the precision of information transmitted from all the CHs would be estimated in BS through the user; when the information is accurate, CH and CM would receive a reward through growing their trust values. Or else they would be punished via decreasing their trust value.

4. Experimental Results Analysis

The simulation analysis of the TAMFO-SC technique takes place interms of network lifetime and energy efficiency.

Table 1 and Fig. 2 provide the number of alive node (NAN) analyses of the TAMFO-SC technique with existing techniques on scenario 1. The results have shown that the TAMFO-SC technique has showcased effective outcomes with the maximum NAN. For instance, with 800 rounds, the TAMFO-SC technique has attained a higher NAN of 100 nodes, whereas the TCCS, LEACH, DEEC, and SEP techniques have obtained a lower NAN of 86, 53, 4, and 8 nodes, respectively. Also, with 1200 rounds, the TAMFO-SC algorithm has attained a maximum NAN of 65 nodes, whereas the TCCS, LEACH, DEEC, and SEP techniques have obtained a lower NAN of 50, 18, 1, and 1 node correspondingly. At the same time, with 1800 rounds, the TAMFO-SC manner has attained an increased NAN of 24 nodes, whereas the TCCS, LEACH, DEEC, and SEP approaches have gained a minimum NAN of 2, 1, 1, and 1 node correspondingly.

DOI: https://doi.org/10.54216/JISIoT.050202

Table 1 NAN analysis of TAMFO-SC model with existing technique under scenario 1

No. of Rounds	TAMFO-SC	TCCS	LEACH	DEEC	SEP
0	100	100	100	100	100
200	100	100	100	100	100
400	100	100	100	100	96
600	100	100	100	92	91
800	100	86	53	4	8
1000	100	70	35	2	1
1200	65	50	18	1	1
1400	41	20	8	1	1
1600	30	7	4	1	1
1800	24	2	1	1	1
2000	17	1	1	1	1

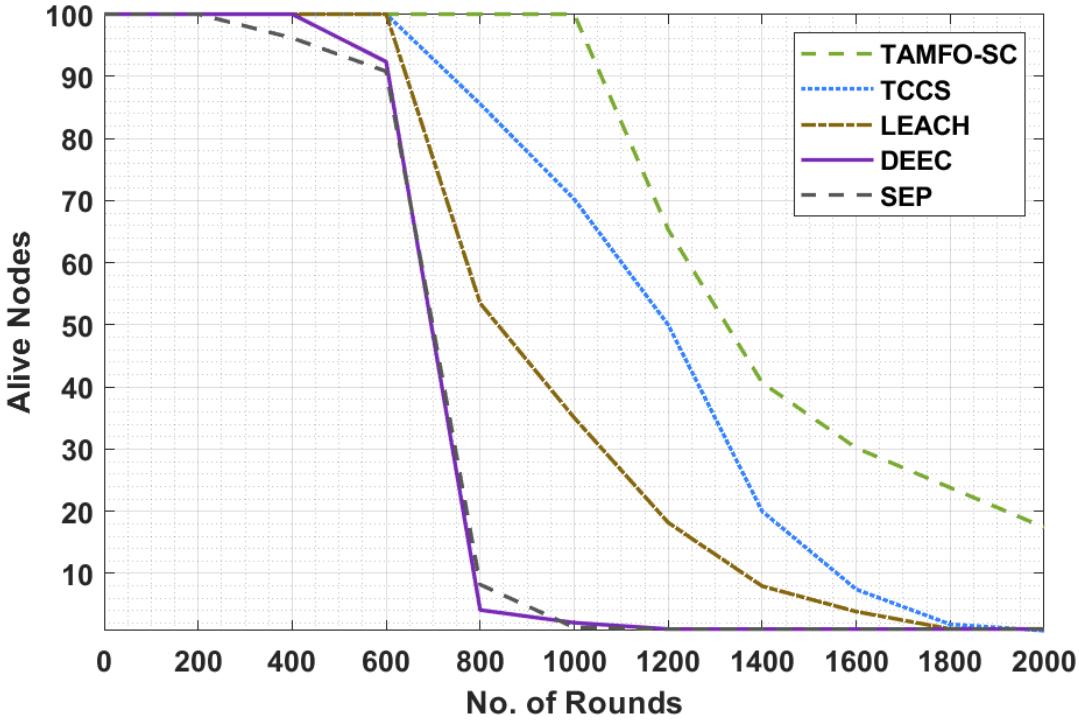

Fig. 2. NAN analysis of TAMFO-SC model under scenario 1

Table 2 and Fig. 3 offer the NAN analysis of the TAMFO-SC algorithm with existing algorithms in scenario 2. The results have shown that the TAMFO-SC technique has outperformed effective outcomes with the maximal NAN. For instance, with 800 rounds, the TAMFO-SC manner has reached a superior NAN of 100 nodes, whereas the TCCS, LEACH, DEEC, and SEP techniques have obtained a lower NAN of 100, 93, 78, and 6 nodes correspondingly. Followed with 1200 rounds, the TAMFO-SC method has attained a higher NAN of 83 nodes, whereas the TCCS, LEACH, DEEC, and SEP techniques have obtained a lower NAN of 80, 57, 2, and 0 nodes correspondingly. Simultaneously, with 1800 rounds, the TAMFO-SC algorithm has attained a higher NAN of 119 nodes, whereas the TCCS, LEACH, DEEC, and SEP systems have achieved a lower NAN of 11, 5, 1, and 0 nodes correspondingly.

DOI: https://doi.org/10.54216/JISIoT.050202

Table 2 NAN analysis of TAMFO-SC model with existing technique under scenario 2

No. of Rounds	TAMFO-SC	TCCS	LEACH	DEEC	SEP
0	100	100	100	100	100
200	100	100	100	99	100
400	100	100	100	100	100
600	99	100	98	99	94
800	100	100	93	78	6
1000	93	87	77	16	3
1200	83	80	57	2	0
1400	64	20	19	1	0
1600	33	11	10	0	0
1800	19	11	5	1	0
2000	12	10	4	1	0

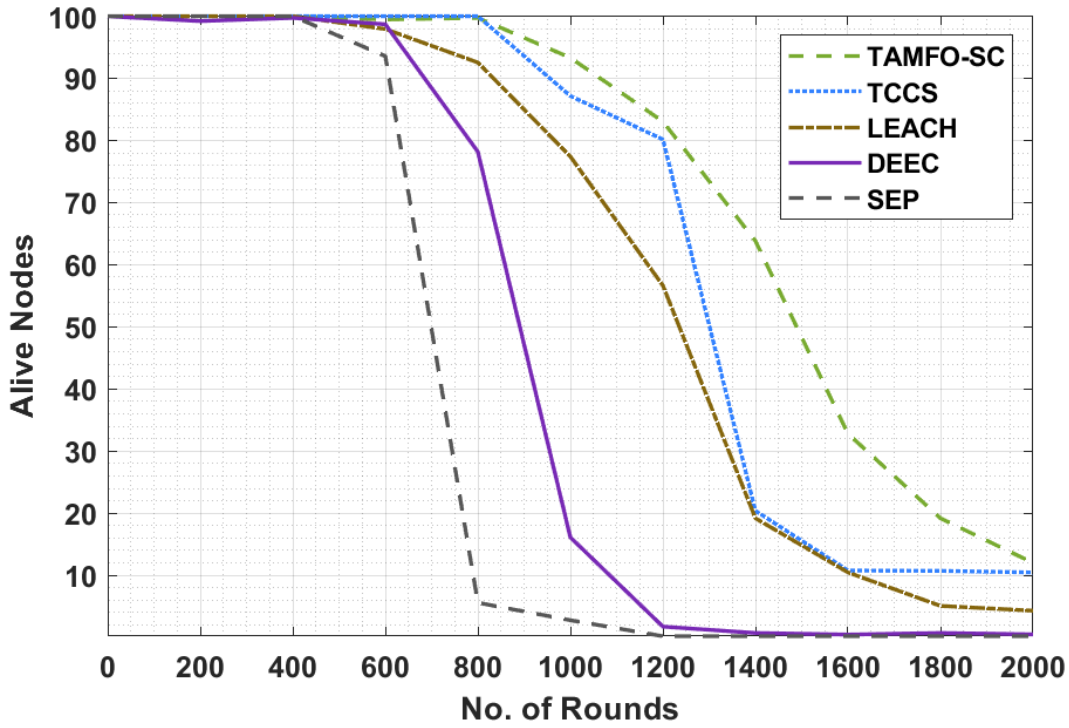

Fig. 3. NAN analysis of TAMFO-SC model under scenario 2

Table 3 and Fig. 4 give the average residual energy (AER) analysis of the TAMFO-SC manner with presented approaches on scenario 1. The outcomes portrayed that the TAMFO-SC method has outperformed effectual outcomes with maximal AER.

DOI: https://doi.org/10.54216/JISIoT.050202

Table 3 AER analysis of TAMFO-SC model with existing technique under scenario 1

No. of Rounds	TAMFO-SC	TCCS	LEACH	DEEC	SEP
0	0.50	0.50	0.50	0.50	0.50
200	0.47	0.42	0.41	0.34	0.34
400	0.37	0.34	0.31	0.21	0.20
600	0.28	0.26	0.23	0.04	0.00
800	0.19	0.16	0.09	0.00	0.00
1000	0.10	0.08	0.02	0.00	0.00
1200	0.05	0.03	0.01	0.00	0.00
1400	0.04	0.02	0.01	0.00	0.00
1600	0.02	0.01	0.01	0.00	0.00
1800	0.01	0.00	0.01	0.00	0.00
2000	0.00	0.00	0.01	0.00	0.00

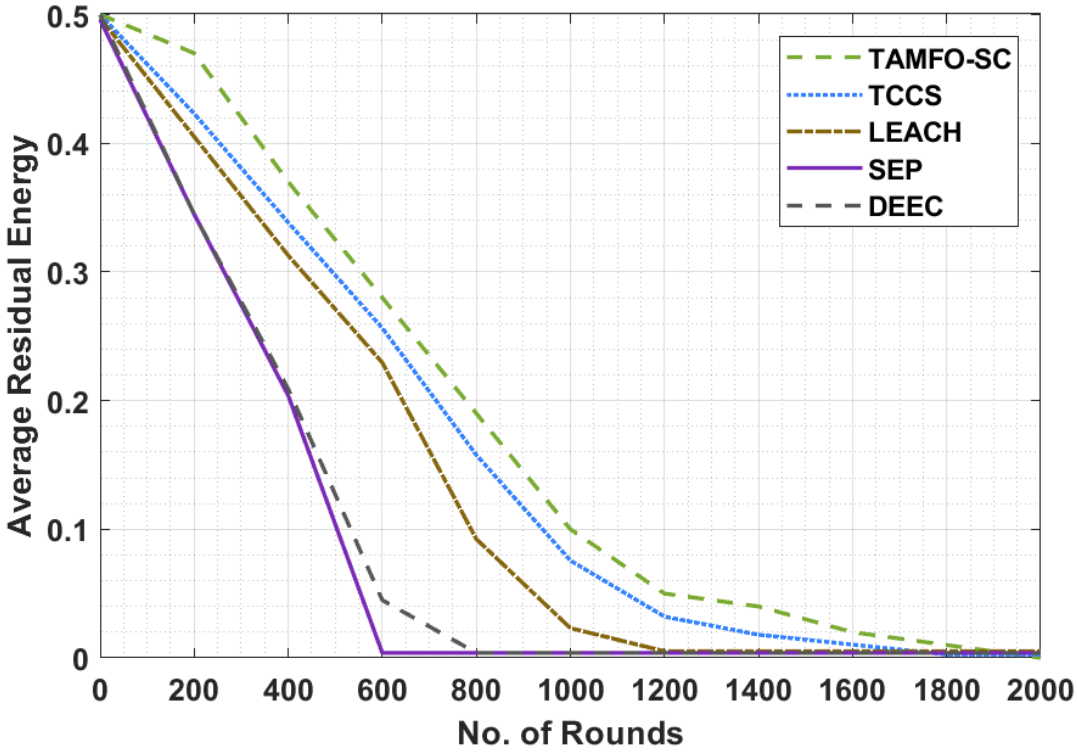

Fig. 4. AER analysis of TAMFO-SC model under scenario 1

For instance, with 800 rounds, the TAMFO-SC approach has attained a superior AER of 0.19, whereas the TCCS, LEACH, DEEC, and SEP algorithms have obtained a lower AER of 0.16, 0.09, 0.00, and 0.00, respectively. With 1200 rounds, the TAMFO-SC technique has attained a higher AER of 0.05, whereas the TCCS, LEACH, DEEC, and SEP schemes have reached a lower AER of 0.03, 0.01, 0.00, and 0.00, respectively. At last, with 1800 rounds, the TAMFO-SC manner has attained a higher AER of 0.01, whereas the TCCS, LEACH, DEEC, and SEP methodologies have obtained a lower AER of 0.00, 0.01, 0.00, and 0.00, respectively.

DOI: https://doi.org/10.54216/JISIoT.050202

Table 4 AER analysis of TAMFO-SC model with existing technique under scenario 2

No. of Rounds	TAMFO-SC	TCCS	LEACH	DEEC	SEP
0	0.50	0.50	0.50	0.50	0.50
200	0.46	0.42	0.39	0.36	0.36
400	0.38	0.34	0.29	0.19	0.19
600	0.28	0.23	0.16	0.04	0.05
800	0.19	0.14	0.04	0.00	0.00
1000	0.09	0.06	0.01	0.00	0.00
1200	0.03	0.03	0.00	0.00	0.00
1400	0.02	0.01	0.00	0.00	0.00
1600	0.01	0.01	0.00	0.00	0.00
1800	0.01	0.01	0.00	0.00	0.00
2000	0.01	0.01	0.00	0.00	0.00

Table 4 and Fig. 5 provide the AER analysis of the TAMFO-SC technique with recent manners on scenario 2. The results depicted that the TAMFO-SC technique has showcased effectual outcomes with the higher AER. For instance, with 800 rounds, the TAMFO-SC technique has attained a higher AER of 0.19, whereas the TCCS, LEACH, DEEC, and SEP manners have gained a lower AER of 0.14, 0.04, 0.00, and 0.00 correspondingly. Besides, with 1200 rounds, the TAMFO-SC approach has attained a higher AER of 0.03, whereas the TCCS, LEACH, DEEC, and SEP techniques have obtained a lower AER of 0.03, 0.00, 0.00, and 0.00, respectively. Lastly, with 1800 rounds, the TAMFO-SC methodology has attained a higher AER of 0.01, whereas the TCCS, LEACH, DEEC, and SEP methods have obtained a lower AER of 0.01, 0.00, 0.00, and 0.00 correspondingly.

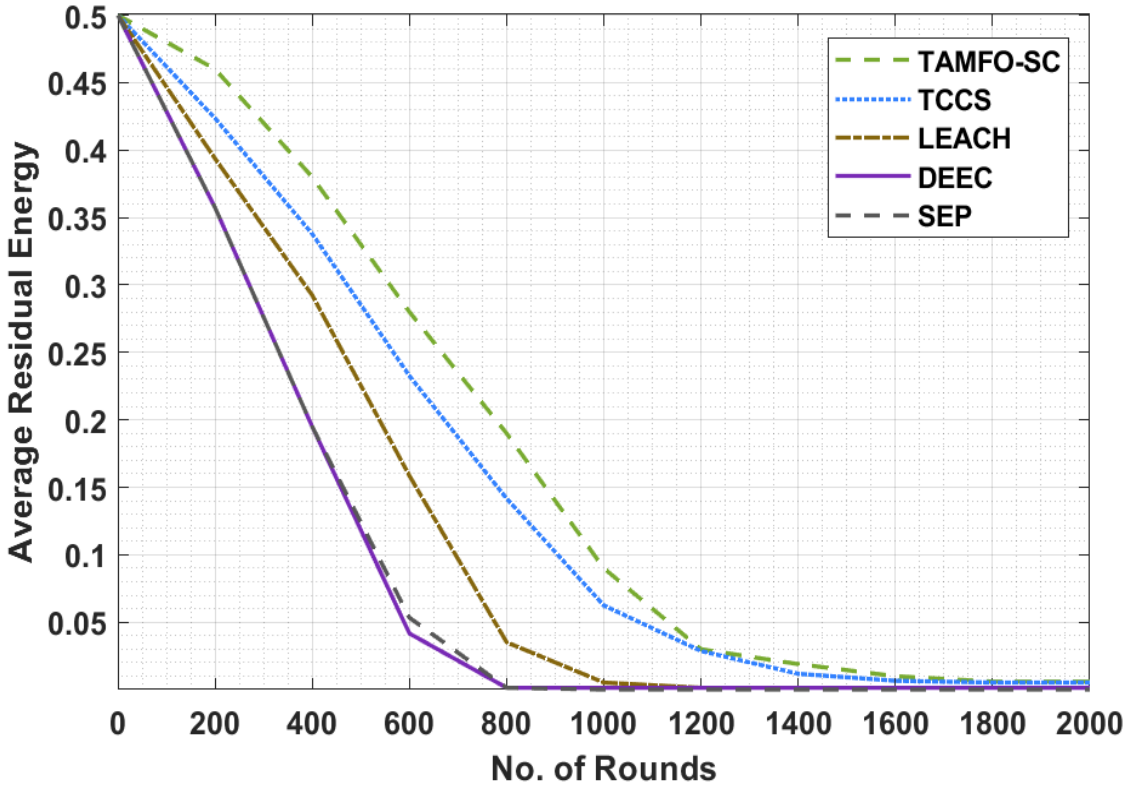

Fig. 5. AER analysis of TAMFO-SC model under scenario 2

DOI: https://doi.org/10.54216/JISIoT.050202

5. Conclusion

This paper has developed a TAMFO-SC technique is to determine the trust level of the nodes and determine the secure CHs. The proposed TAMFO-SC technique initially determines the nodes' trust level, and the node with maximum trust factor can be chosen as CHs. In addition, the TAMFO-SC technique derives a fitness function using two parameters namely RE, and trust level. The inclusion of trust level in the CH selection process helps to accomplish security in WSN. A comprehensive experimental analysis exhibits the promising performance of the TAMFO-SC technique over the other compared methods. Therefore, the TAMFO-SC technique can be utilized to accomplish maximum security and in real-time.

References

[1] Pule, M., Yahya, A. and Chuma, J., 2017. Wireless sensor networks: A survey on monitoring water quality. Journal of applied research and technology, 15(6), pp.562-570.
[2] Xie, H., Yan, Z., Yao, Z. and Atiquzzaman, M., 2018. Data collection for security measurement in wireless sensor networks: A survey. IEEE Internet of Things Journal, 6(2), pp.2205-2224.
[3] Aponte-Luis, J., Gómez-Galán, J.A., Gómez-Bravo, F., Sánchez-Raya, M., Alcina-Espigado, J. and Teixido-Rovira, P.M., 2018. An efficient wireless sensor network for industrial monitoring and control. Sensors, 18(1), p.182.
[4] Wang, B., Gu, X., Ma, L. and Yan, S., 2017. Temperature error correction based on BP neural network in meteorological wireless sensor network. International Journal of Sensor Networks, 23(4), pp.265-278.
[5] Deng, F., Yue, X., Fan, X., Guan, S., Xu, Y. and Chen, J., 2018. Multisource energy harvesting system for a wireless sensor network node in the field environment. IEEE Internet of Things Journal, 6(1), pp.918-927.
[6] Mohamed, R.E., Saleh, A.I., Abdelrazzak, M. and Samra, A.S., 2018. Survey on wireless sensor network applications and energy efficient routing protocols. Wireless Personal Communications, 101(2), pp.1019-1055.
[7] Lombardo, L., Corbellini, S., Parvis, M., Elsayed, A., Angelini, E. and Grassini, S., 2017. Wireless sensor network for distributed environmental monitoring. IEEE Transactions on Instrumentation and Measurement, 67(5), pp.1214-1222.
[8] Qi, J. and Liu, G.P., 2017. A robust high-accuracy ultrasound indoor positioning system based on a wireless sensor network. Sensors, 17(11), p.2554.
[9] Miglani, A., Goel, S. and Bhatia, T.K., 2015. An energy efficient and trust aware framework for secure routing in LEACH for wireless sensor networks (Doctoral dissertation).
[10] Gaber, T., Abdelwahab, S., Elhoseny, M. and Hassanien, A.E., 2018. Trust-based secure clustering in WSN-based intelligent transportation systems. Computer Networks, 146, pp.151-158.
[11] Karthick, S., 2018. TDP: A novel secure and energy aware routing protocol for wireless sensor networks. International Journal of Intelligent Engineering and Systems, 11(2), pp.76-84.
[12] Yang, L., Lu, Y., Liu, S., Guo, T. and Liang, Z., 2018. A dynamic behavior monitoring game-based trust evaluation scheme for clustering in wireless sensor networks. IEEE Access, 6, pp.71404-71412.
[13] Sun, B. and Li, D., 2017. A comprehensive trust-aware routing protocol with multi-attributes for WSNs. IEEE Access, 6, pp.4725-4741.
[14] AlFarraj, O., AlZubi, A. and Tolba, A., 2018. Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, pp.1-11.
[15] Mei, R.N.S., Sulaiman, M.H., Mustaffa, Z. and Daniyal, H., 2017. Optimal reactive power dispatch solution by loss minimization using moth-flame optimization technique. Applied Soft Computing, 59, pp.210-222.

DOI: https://doi.org/10.54216/JISIoT.050202