ISSN (Print): 0974-6846
ISSN (Online): 0974-5645
Indian Journal of Science and Technology, *Vol 12(23), DOI: 10.17485/ijst/2019/v12i23/145375, June 2019*

Trust Aware Energy Efficient Clustering for Secure Packet Transmission in Wireless Sensor Networks

V. Nandalal[1]*, M.S. Sumalatha[1] ,V. Anand Kumar[2] and C. Santhosh Kumar[3]

[1]Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Kuniamuthur, Coimbatore – 641008, Tamil Nadu, India; nandalal@skcet.ac.in, mysansuma@gmail.com
[2]Sri Eshwar College of Engineering, Kondampatti – 641202, Tamil Nadu, India; anandkumar.v@sece.ac.in
[3]Department of Electrical and Electronics Engineering, N S S Polytechnic College Pandalam -689501, Kerala, India; koottungalsanthosh@gmail.com

Abstract

Objective: The proposed work is to improve the network lifetime with secure packet transmission. **Methods/Statistical Analysis:** The proposed system has been suggested here as the TAEBC or the Trust Aware Energy Based Clustering (TAEBC), the introduction of this system has been selected on account of its novel approach in attaining secure packet transmission. The research work suggested here primarily takes into consideration the analysis conducted on the trust score for effectual detection of nodes that appear to be malicious in nature. Choosing and identification of the CH and clustering is executed by deployment of the MOASO or the Multi Objective Anarchies Society Optimization algorithm. The proposed system is to fulfill three main areas which include node degree, residual energy and as well as transmission power. In order to optimize and realize the network's maximum energy potential what has been proposed here is the development and deployment of the MOASO algorithm. This also facilitates CH selection and lifetime for the nodes in a best possible way. **Findings:** The NS-2 simulator has been used for purpose of experimentation and analytical findings. Inferences drawn clearly demonstrate that experimental results have been successful and the suggested TAEBC approach compared with existing system. **Application/Improvements:** The proposed system achieves better end to end delay, energy consumption and Packet Delivery Ratio compared with existing FCR based CH selection method.

Keywords: Anarchies Society Optimization or the ASO and Security, CH or Cluster Head, Wireless Sensor Network also known as WSN

1. Introduction

On the anticipation of having wide application with diverse events associated to emergency response, security monitoring, environmental tracking, WSNs have turned as a growing research fields during the past few years irrespective of manned or unmanned missions. Plethora of intelligent sensors with reduced power is integrated in WSN though it indulges in high power sink. These low power intelligent sensors are accountable for setting up ways among themselves with certain transmission regulations[1]. These wireless sensors are much preferable as they are simple to install, Self-identifiable, self-diagnosable and the best part among them is time realization for coordinating other sensors to construct dynamic self-organized networks. On the other hand, it is controlled with energy constraint, analytical and computational ability, memory and lesser data rate which allows the wireless radio transmission in close proximities[2].

With time the network is established in a hierarchical manner where clustering is the dominating methodology. A vigorous and energy-saving process can be attained through the method of clustering where the nodes are grouped and organized in to small clusters[3]. The heading cluster is accountable for moving further the aggregated data from end nodes to BS. This is forwarded straight from the cluster head or by the down line clusters in a sequential manner. Recent past year's flat architecture was in usage and it is overcome by clustering methodology. This clustering has an edge over flat architecture by

*Author for correspondence

reducing inter node communication, network scalability, bandwidth management and it also allows nodes to nap and becomes an energy saver eventually[4,5]. The apt cluster selection is a mandatory one when you approach cluster based project hence it would directly affect the network performance. Single Criterion cluster (e.g. residual energy) may not be a good choice at times. Failing to choose the suitable cluster would lead to poor performance. In the process of selecting the most appropriate cluster, the distance from other nodes and cluster centered also needed to be taken into account.

High security is mandatory while WSNs gather sensitive and indispensable information. Although, owing to the easy accessibility of wireless channels with dynamic topology, sensor nodes are endangered to diverse attacks such as eavesdropping, node compromising and physical disturbances. The facts might become capricious when they go through these attacks. Consequently, data reliability and reduced energy consumption must be ensured by evolving certain steps[6]. Reliable computing is acquired to identify the attacked nodes in WSNs as a solution to this problem. The nodes that are lower than the desirable standards can be recognized using the sought out route and even it could be used to measure the integrity of nodes.

The newly introduced model in WSNs is Risk-aware Reputation-based Trust (RaRTrust). In order to assess the integrity of a sensor node this rust uses both reputation and risk. It[7,8] further initiates Trust-aware Secure Routing Framework (TSRF) which constitutes features of lightweight and superior ability to with stand assorted attacks. To develop full-fledged prompt security for WSNs it is needed to understand features of attacks over trust aware routing skills. To make available an optimized routing algorithm the system designed uses the collaborative form of trust and QoS metrics for routing eventually.

2. Literature Survey

An indistinct clustering algorithm was designed while the residual energy and the distance for packet transmission were taken into account. Provisional cluster heads are selected based on random number generation on the start. Two main specifications are looked at by this fuzzy method which includes nodes enduring energy and distance to BS. An output variable is produced based on two inputs which lie as competition radius for every cautious cluster node. Transmission of residual energy is done by the provisional cluster hand to ensure if there exists some other tentative cluster node inside its competition radius. Nevertheless, the other mandatory parameter, the node degree is not considered in course of CH election. This might lead to having distant neighbors for CH, consequently intra cluster communication cost increases sharply and the lifetime of the network is decreased[9].

The structured the wireless sensor network and deployed the Enhanced PSO-Based Clustering Energy Optimization (EPSO-CEO) algorithm. Determination of CH has been finished by utilizing Particle Swarm Optimization also known as PSO algorithm specifically for limiting WSN power utilization. Research and study here includes deployment of the multi-hop correspondence protocol utilized to enable information transmission amongst nodes to CH (intra-cluster directing) and CH with respect to main objective. Information conglomeration is finished by the CH in every cluster for main objective of conserving remainder of energy and thus optimizing energy use. The reenactment result demonstrates that the structured clustering plan gives improved execution so as to limit the complete expended vitality and increment the lifetime of WSN[10] includes the structured planning and usage of a developed Pareto streamlining based way to handle the issues identified with the recognizable proof of ideal system design. For assessment, created model has determined requirements as tally of CH, grouped hub verification, interface quality among CMs. To choose finest ideal result, author tackled detailed issue via Multi-Objective Evolutionary Algorithms also known as MOEA. Additionally, the protocol that has evolved here was assessed with respect to the system lifetime and proficient energy use[11].

A significant amount of research has been directed on powerful techniques for distinguishing irregular nodes and alleviating the levels of security, validity, and unwavering quality of WSNs a novel Reputation-based Framework for Sensor Networks also known as RFSN which utilized a guard dog instrument to manufacture trust rating. Inside RFSN structure, Beta Reputation framework for Sensor Networks (BRSN) that utilized Bayesian definition was utilized. At that point, information combination is carrying out on weighted information readings, in this way decreasing the effect of nodes that cannot be trusted and appear untrustworthy[12].

The planned an innovative but practical non-notoriety based plan called DRBTS or Distributed Reputation based Beacon Trust System for barring noxious BNs also known as Beacon Nodes that give false area data. With regards to DRBTS, each BN screens its one-jump neighborhood for getting into mischief BNs and gives data by keeping up and trading a neighbor's non-notoriety. Be that as it may, these techniques just spotlight on the security of the stay. In addition, they need more calculation and vitality[13].

3. Proposed Methodology

3.1 Network Model

As part of the sensor arrangement, the sensor nodes therein are arbitrarily conveyed in a roundabout zone having a radius as R. The system model can be portrayed as undirected availability diagram G(S, E), where S is arrangement of all sensor nodes, E(i, j) is arrangement of remote connection between hub I and hub j. Sensor nodes are characterized by their homogeneity and stationary. There is just a single BS which lies outside the system. Every one of the nodes is vitality compelled with a uniform beginning vitality distribution. Every node has certain amount of transmission levels that are usually fixed and power control capacity to shift their transmission control. As per the separation or approximate distance to target nodes, however the adjustment between source nodes allows change of transmission control respectively.

3.2 True Value Computation

So as to assess the trust amongst nodes, a wireless or remote situation with nodes and at first the ones considered with trust value as being 0. The planned framework computes trust score for individual hub dependent on accompanying two limitations. Initially, Nodes which really sending their affirmation to neighbors at whatever point they got the parcels are considered as initial gathering. Subsequently, nodes which dropped parcels are measured as gathering 2 nodes. Presently beginning trust score is processed utilizing Eq. (1) that speaks to rate of authentic recognize.

$$TS_{(1,i)} = \frac{\left[W_1 * \left(\frac{ACK}{RP} * 100\right)\right]}{[W_1]} \tag{1}$$

where, W1, W2 and W3 are considered as ascertained weights that are provided to distinctive trust scores, TS(1,i) signify primary trust score of rate for ith hub, ACK speak to quantity of affirmations transmit to neighbors and RP shows quantity of bundles got from neighbors. Subsequent trust score is registered utilizing Eq. (2) which figures packet dropped.

$$TS_{(2,i)} = 100-\left(\left(\frac{DP}{TDP}\right)*100\right),\ t_1 \le t \le t_2 \tag{2}$$

where, 〖TS〗_((2,i)) specifies second trust score in rate for ith node, DP shows quantity of bundles dropped and TDP demonstrates complete amount of parcels dropped in system and t is worldly limitation to verify time limits t1 and t2 for lower and maximum cutoff points of time interim. At long last, we compute the general trust score of specific hub I by utilizing the Eq. (3).

$$TS_i = \frac{\left(TS_{(1,i)} + TS_{(2,i)}\right)}{2} \tag{3}$$

Here, assuming that TS_i specifies general trust score for hub I, 〖TS〗_((1,i)) speaks to main trust score for hub I and 〖TS〗_((2,i)) specifies second trust score for hub I.

For the following research, we allocate limit dependent on mean estimation of general trust score for every one of nodes available in system situation. To begin with, locate the mean esteem utilizing the general trust scores using Eq. 6 in research work.

$$TM = \sum_{i=1}^{n} TSi/n \tag{4}$$

where,

TM -Trust score mean value

TS_i -Trust scores summation

n -Number of nodes

TM is threshold to determine malicious node from network. At last, identify all malicious nodes from network and isolate malicious nodes $M_1, M_2, \ldots M_K$.

3.3 Cluster Head Selection

For this particular section of the research, choosing of CH has been executed by deploying the MOASO or the Multi-Objective Anarchies Society Optimization algorithm. This has been done in a manner that is optimal and within the performance of network. Suggested work here entails that the residual energy, node degree as well as the transmission power are assumed and reviewed as being important as well functionally objective in nature.

3.3.1 Multi Objective Model

3.3.1.1 Remaining Energy

Residual energy of nodes is then calculated and estimated by use of the formula stated. The furthermore in the duration of the solution designed it may be calculated by using the formulas as stated in the equation:

$$\text{Remainingergy} = \text{initialenergy} - \text{consumedenergy} \tag{5}$$

3.3.1.2 Node Degree (N_{deg})

Find the neighbours (node degree) N(v) of each node v , within R_v .

$$N(v)=\{ v' \,|\text{distance}(v, v') \le R_v \tag{6}$$

3.3.1.3 Transmission Power (Tx)

Then find transmission power using formula below:

$$P_{AB} = R^2 \tag{7}$$

where,

P_{AB} - minimum required transmission power from node A to getaway B,

R - Transmission range in (m).

Weight of each node can be calculated using weight based clustering method.

$$W = w_1 R_e + w_2 Tx + w_3 N_{deg} \tag{8}$$

$$w_1 + w_2 + w_3 = 1 \tag{9}$$

where,

w_1 , w_2 ,w_3–weighting factor

Herein nodes common feature is the weight W and the factors $\omega 1$ … $\omega 3$ are essentially weight factors with a value that ranges between 0−1. The factors that taken in to consideration here are essentially the scale for the values that are secured based on the network parameters. These are necessary as the summative value is equal to exactly 1. Additionally, briefly discussed is the role of node parameters deployed during the selection process of cluster head also known as CH.

3.3.2 Cluster Head Selection using Multi Objective Anarchies Society Optimization (MOASO) Algorithm

Depending on the residual energy, node degree and transmission control, choosing CH is executed by deploying the MOASO algorithm. For solution space S, $f : S \rightarrow R$ is function to be minimized in S. By assuming this, consider N member (number of nodes), has been thoroughly searched by a territory that is not known (solution space) for demonstrating finest place to live (i.e., overall minimum of f on S). X_i(k) offers location of ith member in kth iteration; X∗(k) specifies finest position specified by entire members in kth iteration; and Gbest is best position (CH) experienced by ith member during first k iterations.

Hence, at that point, the wellness of each part (node) is resolved. Here residual vitality, node degree and transmission power are considered as a goal work. As indicated by the determined wellness value and examination with X∗(k), P_i^{best} and G^{best}, the development approach and another situation of the part will be resolved. After a sufficient number of cycles, in any event one of the individuals will achieve the ideal position[14].

3.3.2.1 Movement Policy Based on Current Positions

Principal development strategy for ith member in kth iteration [$MP_i^{current}$ (k)] is embraced dependent on present position. Fickleness Index FIi(k) for part I in emphasis k is utilized to choose development strategy. This list estimates the fulfillment of present position of ith part contrasted and other individuals' positions. If target capacity is certain in S, Fickleness Index is communicated as accompanying structures:

$$FI_i\left(k\right) = 1 - \propto_i \frac{f\left(X^*\left(k\right)\right)}{f(X_i\left(k\right)} - (1 - \propto_i) \frac{f\left(P_i\left(k\right)\right)}{f(X_i\left(k\right)} \tag{10}$$

$$FI_i\left(k\right) = 1 - \propto_i \frac{f\left(G\left(k\right)\right)}{f(X_i\left(k\right)} - (1 - \propto_i) \frac{f\left(P_i\left(k\right)\right)}{f(X_i\left(k\right)} \tag{11}$$

Herein, $\propto_i$ is non-negative number in [0,1]. Along these lines, Fickleness Index is number in scope of [0,1]. As per estimations of Fickleness Index, ith member would choose his/her next position. If F I_i (k) is smallest, ith member has best position among all individuals. It is smarter to choose development arrangement dependent on X^* (k). In any other circumstantial situation the ith member is seen to be characterized with a movement that is erratic. Hence here movement policy for ith member is as per value F I_i (k) and may be shown as per the following:

$$[MP_i^{current}\left(k\right)] =$$

$$\begin{Bmatrix} \textit{moving towards } X^*\left(k\right) 0 \le FI_i\left(k\right) \le \alpha_i \\ \textit{moving toward a random } X_i(\left(k\right) \alpha_i \le FI_i\left(k\right) \le 1 \end{Bmatrix} \tag{12}$$

3.3.2.2 *Movement Policy based Positions of Other Members*

Second development arrangement with regards to ith member in kth iteration $[MP_i^{society}(k)]$ is received dependent on places of different individuals. Albeit every part should move toward G^{best} coherently, the development of the part isn't unsurprising because of the revolutionary idea of the part and may advance toward another network part. Hence, the outside abnormality list entails that E I_i (k) for ith member in kth iteration thus may be computed as per the following:

$$EI_i(k) = 1 - e^{-\theta_i[f(X_i(k)) - f(G(k))]} \tag{13}$$

$$EI_i(k) = 1 - e^{-\delta_i D(k)]} \tag{14}$$

where θ_i and δ_i are certain numbers, D(k)is a measure of proper scattering coefficient of variety CV(k). Equation characterizes the separation of network part I from Gbest. On the off chance that the network part is near Gbest, it will have a more rationale conduct. Else, it demonstrates an anarchic conduct dependent on rebellion. Above Equation characterizes a decent variety file in network which has an immediate association with the assorted variety of the network individuals. For the situation that this record is chosen, the network individuals should carry on more coherently and they are less broadened. In this manner, with thought of a limit for EI*i* (k) , it is conceivable to characterize the development strategy dependent on the places of different individuals as pursues:

$$[MP_i^{society}(k)] = \begin{Bmatrix} moving\ towards\ G^{best}\ 0 \le EI_i(k) \le threshold \\ moving\ toward\ a\ random\ X_i((k)\ threshold \le EI_i(k) \le 1 \end{Bmatrix} \tag{15}$$

Closer limit is to zero, more irrational part developments. As edge unites individuals act intelligently.

3.3.2.3 *Movement Policy Based on Previous Positions*

Third is development strategy for ith member in kthiteration $[MP_i^{past}(k)]$ is embraced dependent on the past places of the individual part. So as to choose this development arrangement, the situation of ith member in kth iteration is compared to Pbest i. If situation of part is near P_i^{best} , t the part acts all the more consistently. Something else, the part indicates strange conduct. To decide the development arrangement dependent on past positions, the inside anomaly list II_i (k) for ith part in kth cycle is characterized as pursues:

$$II_i(k) = 1 - e^{-\beta_i[f(X_i(k)) - f(P_i(k))]} \tag{16}$$

where, bi is positive number. Alike of previous policy, with threshold selection for IIi(k), movement policy is distinct sourced on prior positions as follows:

$$[MP_i^{past}(k)] = \begin{Bmatrix} moving\ towards\ P_i^{best}\ 0 \le II_i(k) \le threshold \\ moving\ toward\ a\ random\ X_i((k)\ threshold \le II_i(k) \le 1 \end{Bmatrix} \tag{17}$$

Depending on how close the threshold is towards zero, member movements may seem to be irrational, random and illogical. However the closer the threshold converges to 1, member movement would be that more sequential and logical.

3.3.2.4 *Combination of Movement Policies*

Selection of final movement policy, a combination of three policies has been elucidated upon previously. Post computation of movement policies, every member essentially must almost consciously try to fuse these policies together using a methodology and gradually shift towards a position that is new. A simple but effective way is selection of a policy that has the best answer. Thereafter the next best solution is a sequential combination of movement policies with one another also known as the sequential combination rule. There are two possible outcomes while using this crossover method one wherein it may be utilized for incessant issues inherent and coded as chromosomes, or sequentially utilized as a combination of the movement policies.

Algorithm 1: Multi objective ASO Algorithm

Input: N number of nodes
Output: Optimal CH selection

1. Initialize the N nodes, member position and set of iterations counter I=0
2. Generate M initial solutions and evaluate their fitness values (Remaining energy, node degree and transmission power)

```
3. While (termination criteria are not satisfied)
4. Determining the values of $X^*$ (k), $P_i^{best}$ and , $G^{best}$
5. For i = 1:M
6. Computing F $I_i$ (k)
7. If F $I_i$ (k) is less than threshold $X_i$ (k) , then $X_i$ (k) moves towards $X^*$ (k)
8. Else $X_i$ (k) moves towards a random member
9. End if
10. End for
11. For i = 1:M
12. Computing E $I_i$ (k)
13. If E $I_i$ (k) is less than threshold $X_i$ (k) , then $X_i$ (k) moves towards $G^{best}$
14. Else $X_i$ (k) moves towards a random member
15. End if
16. End for
17. For i = 1:M
18. Computing I $I_i$ (k)
19. If I $I_i$ (k) is less than threshold $X_i$ (k) , then $X_i$ (k) moves towards $P_i^{best}$
20. Else $X_i$ (k) moves towards a random member
21. End if
22. End for
23. For i = 1:M
24. Updating the position by combining the movement policies
25. Calculating the fitness values (Remaining energy, node degree and transmission power) for the members of society
26. End for
27. End while
28. Report the best solution (Optimal CH)
29. End
```

Based on the remaining energy, node degree and transmission power the CH are selected for packet transmission.

4. Experimental Results

Here, performance of anticipated Trust Aware Energy Based Clustering (TAEBC) is evaluated and contrasted with existing methods such as FCR method methods. The experiments are performed with NS-2 simulator. The existing and proposed methods are compared based on energy consumption and E2E delay PDR.

4.1 E2E Delay

E2E delay on network specifies time taken by packet to be broadcasted over network from source to destination.

Figure 1 illustrates, the comparison between the existing FCR based CH selection and proposed Trust Aware Energy Based Clustering (TAEBC) method for E2E delay. Nodes are transformed from 20 to 100 and E2E delay is graphically plotted for nodes in milli seconds (ms). Simulation result demonstrates that anticipated TAEBC approach attains lesser E2E delay than prevailing FCR based CH selection approach.

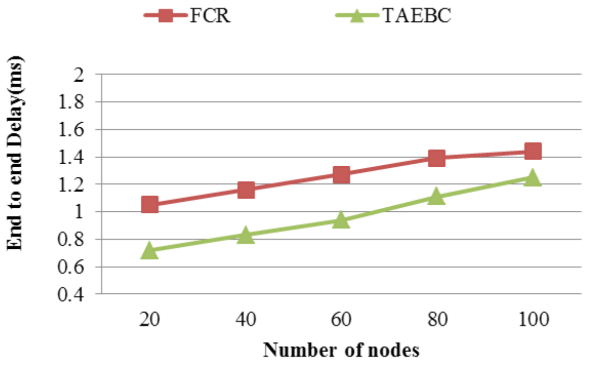

Figure 1. End to end delay comparison.

4.2 Energy Consumption

Average energy here infers to the energy that has been consumed in the network for necessary transmission, receipt or the process of forwarding operations of packet to node and this is for specific time duration

$$Energy\ \left(e\right)=[\left(2*pi-1\right)\left(e_t+e_r\right)d \tag{18}$$

where, pi is data packet, e_t is energy for packet transmission i, e_r is energy for receiving packet i and d is distance amongst destination node and transmission node.

Performance of anticipated TAEBC approach is compared with the existing FCR based CH selection method based on energy consumption. Node is plotted over x axis and energy consumption is plotted over y axis. It depicts that prevailing FCR based CH selection approaches offer superior energy consumption where anticipated TAEBC provides lesser energy consumption.

5. Packet Delivery Ratio (PDR)

The ratio between the numbers of data packets successfully delivered to the destination and the number of packets transmitted by the source.

$$\text{PDR}=\frac{\text{Number of packets attained}}{\text{Number of packets transmitted}} \tag{19}$$

From Figure 3, it is depicted that comparison of PDR using existing FCR based CH selection method and proposed TAEBC approach. Node is plotted over x axis and PDR is plotted over y axis. It depicts that prevailing FCR based CH selection method provide lower packet delivery ratio whereas the proposed TAEBC provide higher packet delivery ratio.

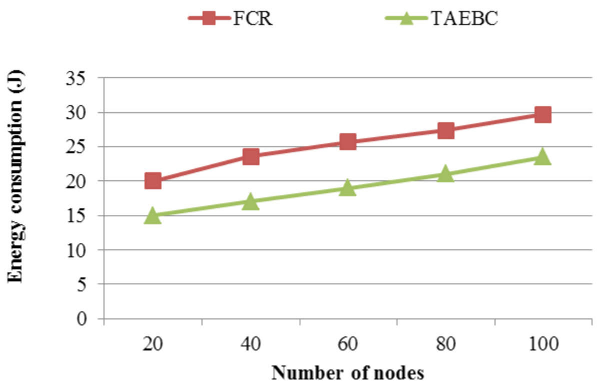

Figure 2. Energy consumption comparison.

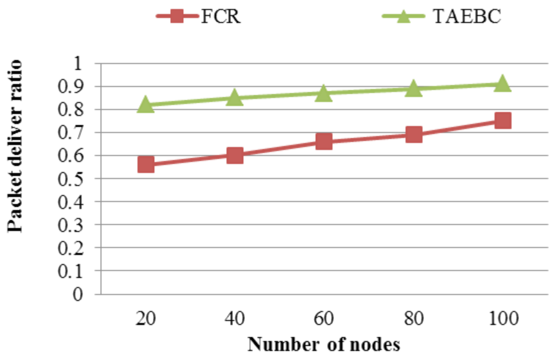

Figure 3. PDR comparison.

6. Conclusion

The research and study that has been conducted here has effectively introduced the Trust Aware Energy Based Clustering or the TAEBC approach for acquisition of secure packet transmission characterized by an energy efficiency level that is relatively high. During the primary phase every node's trust score has been carefully computed to facilitate the determination of malicious node and their detection. Malicious nodes then have been eliminated from the network and the process of clustering has then been executed. Selection of CH or cluster head has been made possible by deployment of the Multi Objective Anarchies Society Optimization or the MOASO algorithm depending on residual energy, node degree and the transmission power. This results in enhancing the life time as well as in optimizing energy utilization of the network. Inferences drawn on the basis of experiments clearly show that suggested TAEBC approach performs better and its execution results in achieving an E2E delay PDR and optimal usage of energy when compared with existing systems.

7. References

1. Jenifer Y, Mukherjee B, Ghosa, D. Wireless sensor network Survey. Computing. 2008; 52:2292–330. https://doi.org/10.1016/j.comnet.2008.04.002.
2. Phuntsog T, Kumar AA. Design issues and various routing protocols for wireless sensor network. Proceedings of National Conference on New Horizons in IT - NCNHIT 2013; 2013. p. 65–7.
3. Aslam N, Phillips W, Robertson W, Sivakumar S. A multi-criterion optimization technique for energy efficient cluster formation in wireless sensor networks. Information Fusion. 2011; 12(3):202–12. https://doi.org/10.1016/j.inffus.2009.12.005.
4. Zhu J, Lung CH, Srivastave V. Hybrid clustering technique using quantitative and qualitative data for wireless sensor networks. Ad-hoc Networks. 2015; 25:38–53. https://doi.org/10.1016/j.adhoc.2014.09.009.
5. Lin D, Wang Q. An energy-efficient clustering algorithm combined game theory and dual-cluster-head mechanism for WSNs. IEEE Access; 2019. https://doi.org/10.1109/ACCESS.2019.2911190.
6. Chen Z, Tian L, Lin C. Trust model of wireless sensor networks and its application in data fusion. Sensors. 2017; 17(4):703. https://doi.org/10.3390/s17040703. PMid:28350347. PMCid:PMC5421663.
7. Labraoui N, Gueroui M, Sekhri LA. Risk-aware reputation-based trust management in wireless sensor networks. Wireless Pers. Communication. 2015; 87:1037–55. https://doi.org/10.1007/s11277-015-2636-3.

8. Duan J, Yang D, Zhu H, Zhang S, Zhao J. TSRF: A trust-aware secure routing framework in wireless sensor networks. International Journal of Distributed Sensor Networks. 2014; 10 (1):209436. https://doi.org/10.1155/2014/209436.
9. Bagci H, Yazici A. An energy aware fuzzy unequal clustering algorithm for wireless sensor networks. IEEE International Conference on Fuzzy Systems; 2010. p. 1–8. https://doi.org/10.1109/FUZZY.2010.5584580.
10. Vimalarani R, Subramanian, Sivanandam SN. An enhanced PSO-based clustering energy optimization algorithm for wireless sensor network. The Scientific World Journal; 2016. https://doi.org/10.1155/2016/8658760. PMid:26881273. PMCid:PMC4736907.
11. Elhabyan R, Shi W, St-Hilaire M. A Pareto optimization-based approach to clustering and routing in Wireless Sensor Networks. Journal of Network and Computer Applications. 2018; 114:57–69. https://doi.org/10.1016/j.jnca.2018.04.005.
12. Ganeriwal S, Balzano LK, Srivastava MB. Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks. 2008; 4:1–37. https://doi.org/10.1145/1362542.1362546.
13. Srinivasan A, Teitelbaum J, Wu J. DRBTS: Distributed reputation-based beacon trust system. Proceedings of the IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, IN, USA; 2006. p. 277–83. https://doi.org/10.1109/DASC.2006.28. PMid:16933740.
14. Bozorgi A, Bozorg-Haddad O, Chu X. Anarchic Society Optimization (ASO) algorithm. Advanced Optimization by Nature-Inspired Algorithms. Springer, Singapore; 2018. p. 31–8. https://doi.org/10.1007/978-981-10-5221-7_4.