ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20230307000418
Original scientific paper

Query Based Location Aware Energy Efficient Secure Multicast Routing for Wireless Sensor Networks Using Fuzzy Logic

Karthick CHANDRASEKARAN*, Kathirvel CHINNASAMY

Abstract: In Wireless Sensor Networks (WSNs), balancing authentication and energy is a major concern while deploying for wireless applications. Due to the presence of attackers, node consumes excessive energy for packet replication or transmission. In existing work, it is observed that attention was not done on balancing energy and data authentication. Location aided routing will also support for achieving high network lifetime. Fuzzy decision approach was widely used in sensor network for ensuring quality of routing and transmission. In the proposed work, Fuzzy enhanced query based secure energy efficient multicast routing is implemented. Query based location based cluster formation is done for quick packet arrival. Optimal multicast routes are found to forward the packets with reliability. The reliable routes are identified using reliable index. Fuzzy decision model is integrated to provide secure and energy based network model for packet transmission. Network Simulator (NS2.35) is used for simulation for analyzing the performance of proposed protocol in terms of various network parameters.

Keywords: cluster formation; energy model; fuzzy decision model; optimal multicast route; query based location aided routing; trust model for security

1 INTRODUCTION

The human life is influenced by wireless sensor network in every moment. The network gives solutions to all issues in effective manner. WSN has been deployed everywhere like environment monitoring, healthcare, industry and commercial applications. WSN is also helpful for developing Internet of Things (IoT) applications [1, 2]. Sensor nodes mainly depend on batteries. Charging or replacement of batteries is not possible in some scenarios. Packet transmission in WSN is an important aspect while considering energy and security. It is very important to focus on energy related issues for data collection and transmission.

Clustering technology plays an important role in WSN in improving energy efficiency to prolong network lifespan. Sensor region is divided into cluster zones based on defined parameters. Choosing Cluster Head (CH) is challengeable in tracking and balancing the energy conservation during routing process. In such scenarios, CH gathers information from cluster members and forwards it to sink node. If the CH energy level falls below the threshold value, it is important to choose the other replace node in a certain period.

Location based routing is also one of the key issues in WSN. By implementing localized routing, network size will be scalable and overhead can be reduced based on geographical position of nodes. Each node must identify the location of other nodes by Geographical Positioning System (GPS). The location of single hop neighbour node must be known by every node and the source node must also track the location of sink node. The information about the location of node is sensed by many techniques like proximity or triangulation methods. The exact location information is required for all wireless applications. The location routing is required to assist energy and security during the data transmission from CH to CMs.

Energy efficient multicast routing is also an important consideration which will support in providing effective authentication of data and route reliability. Multicast route provides scalability and flexibility for improving network lifetime. If the primary route is out of state, packets will be directed through secondary route for packet arrival at sink node. In many routing mechanisms, energy is wasted due to unbalanced routes and nodes which will affect the network lifetime. Energy conservation is very important consideration for improving the efficiency. In such networks, issues in data aggregation and routing [3] were found for saving energy in WSN. The concept of fuzzy based aggregation approach was introduced with optimization algorithm. Due to huge network region, there was a chance of packet duplication. It may reduce the energy consumption while replaying of packets. Due to heterogeneous nature, energy consumption may be highly consumed. In such scenarios, bluetooth assisted sensor nodes for IoT applications were implemented [4].

Reliability of node is computed in such schemes in terms of trust, packet forwarding and energy conservation. But in some cases, route reliability is not able to attain network efficiency due to the presence of unreliable nodes. Trust mechanism is required to detect and avoid malicious activities or node to protect the network from attackers.

In this research work, various queries like energy, route, security and location are raised and resolved using the proposed protocol with fuzzy decision model providing effective data gathering, energy efficiency and secured routing.

2 LITERATURE REVIEW

Kashif Naseer Qureshi et al. [5] developed the random clustering approach through gateway routing method. Cluster region was created and cluster head load was reduced to monitor the energy level of cluster members. Based on centroid location, the geographical poisition of CH was adjusted to balance load and energy.

Abhishek Jain et al. [6] developed the trust vector based intrusion detection model to handle the active and passive attackers using risk module to analyze the impact of attackers. Data gathering approach was used to form cluster. The reliable nodes are found using the trust model. Based on intrusion detection system, data transmission policy will be approved for secure data transmission.

Girish et al. [7] demonstrated the reliable location based energy aware routing to fight against the routing attacks. Misbehaving nodes are identified and isolated

from the network to free the network from attackers.The computational resources are consumed unlimitedly because of unreliable route selection. For the selection of reliable node, cost based hop routes and stability and mobility metric were computed and used for performance analysis. The intruders were identified through trust worthy parameter and reliable paths were chosen for high delivery rate. Both passive and active attackers were avoided in the network due to optimum network routing algorithm which will enable nodes to isolate the communication of the attackers.

Xiuniao et al. [8] presented the new optimization scheme with multi-objective algorithm to choose cluster member nodes and cluster head based on energy consumption rate and minimum hop distance. The distance between the intra cluster region was reduced. Based on cuckoo approach and multi-objective approach, the energy wastage was reduced because of selection of optimal routes and CH. The fitness function was evaluated based on balancing quality of service metrics and optimal solutions for network issues.

Chen et al. [9] analyzed the sensor network routing issues and introduced the concept of control based energy efficient routing through quantum approach. Data readiness and compatibility were evaluated in the presence of attackers. The authors reviewed and implemented the integration of quantum processor and network optimization problem to encode the issues and solved the issues of energy conservation in the network.

Rehman et al. [10] introduced the concept of key management scheme based on polynomial approach for securing data transmission in WSN. Whenever the network changes happen, polynomial approach was adopted to protect the data and support network scalability. The key pool size was reduced to improve the network lifetime.

Meysam and mohammedreza [11] developed the trust model using gray system method to improve network lifespan in IoT. Here the concept of clustering was adopted to ensure route reliability. The trust management module was adopted to choose optimal routes. Both direct and indirect trust vector was calculated to ensure node reliability. The basic structure of LEACH was modified to support trust routing. The framework was developed with scheduling, clustering and route advertisment. False nodes are identified based on packet dropping rate and replaying of packets.

Selvi et al. [12] developed a security model based on trust vector to support secure data communication in sensor networks. The trust rate verification approach was used for detecting malicious nodes and best routes are identified using decision based routing algorithm. Trust enhanced model was also deployed for monitoring energy level of sensor node during data transmission process.

Gopinath et al. [13] presented the stability based secure energy efficient multicast routing scheme for WSN. Here the network model and routing assumptions were made for effecitve data transmission. Stable routes are determined and used for increasing throughput. Security model and energy consumption model were integrated to balance network security and energy efficiency.

Rangappa and Dyamanna [14] presented the optimization algorithm to ensure energy efficiency in WSN. The algorithm limits the unauthorized node mobility in the network zone and decreases the energy consumption. The routing strategy and packet transmission technology were modified according to optimization approach which helps in reducing the energy consumption.

Eswaramoorthy et al. [15] proposed the location aware directional flooding algorithm to increase the energy efficiency. The delay and packet loss rate were decreased due to decision based reliable route and sleep nodes. The reliability and latency were improved using flooding mechanism to improve network performance.

Kantharaju and Sanjeev [16] introduced the energy based reliable multi-objective hybrid optimization algorithm for identifying and isolating misbehaving nodes. The fitness parameter was evaluated and identified to increase node identification and enhance the performance of multi-hop routing.

Xiang Wang et al. [17] explored query based location aware geographic routing protocol to increase the node lifetime. The monitoring area was divided into clusters to decrease the communication overhead. The distance between cluster member and grid center was measured from residual energy and nearby adjacent cluster heads. The next hop routes were chosen based on remaining energy and distance between the cluster members.

Kavana [18] presented the multi-hop routing protocol based on secret sharing approach. The work was focused on improving residual energy and multi-hop data security. Based on position of nodes, the zone was divided into internal and external zones. Based on neighbour node location, cluster region is formed. The secret sharing security mechanism was integrated to secure the node with high data integrity. The statistical analysis was derived to analyze the route to reduce traffic issue. Based on data analyst and network integrity, the work was introduced with Internet of Things.

Banerjee and Ghosh [19] presented a weight based secure energy efficient routing to improve the network lifetime. Stable routes were found based on stability index and they protect the data from the attackers. In the presence of current session, energy drain ratio was not modified except the new established route. The route re-establishment phase was avoided due to high message cost. The mutliple routes were identified with cost metric for each session.

Arzoo et al. [20] explored the reliable framework for secure and energy efficient routing in sensor network. Here the multicast route was adopted to improve the packet delivery rate. Sensor nodes were identified and optimal multi-cast routes were found. Least hop distance and data handling capacity decide the data transmission from source to sink. Clear to Send (CTS) and Request to Send (RTS) packet transmission was used to identify the collision between the nodes.

Saini et al. [21] developed the enery consumption model using dynamic route adjustment model to balance the energy and route stability in the presence of attackers. This approach was used to rectify the issues of mobility, unstability and route failures to improve the route efficiency. Energy model was integrated to monitor the energy level at transmitter and receiver [22].

The paper is organized into five sections. In the first section, introduction was given based on security and energy related issues in WSN. In the second section, the

previous work was given and the lags were identified. In the third section, proposed protocol was implemented to balance network security and energy. Fourth section provides simulation results and discussion. Last section concludes and proposes the future work.

3 PROPOSED PROTOCOL

In the proposed protocol, the following queries are raised and used to balance the security and energy in the proposed protocol.

- Energy query - If energy gets depleted, how to prolong the network lifespan
- Stability query - If node is not stable, how the reliable neighbour node will be chosen.
- Reliability query - If the route reliability is broken, what is the alternation to choose other route.
- Security query - If data is not protected, how the security provision will be provided for data protection.

These queries are resolved using our proposed protocol through fuzzy enhanced reliable multicast routing model. The following phases are proposed to stabilize the routing.

1. Cluster formation and Cluster Head election
2. Optimal Multicast Route discovery phase and energy model
3. Reliable routing scheme
4. Fuzzy decision model

The following assumptions are made to improve the network lifetime while reducing energy consumption.

1. Each node has unique identity number, and all nodes are deployed randomly in network region and it contains less mobility.
2. Cluster formation is done based on node location and reliability algorithm.
3. Main Cluster Head (MCH) and Deputy Cluster Head (DCH) have more energy resources and higher stability than other nodes.
4. The coverage region is measured based on distance between source and sink node.
5. Reliability metric and energy metric are kept confidential, and they are maintained by CH to identify the reliable cluster members and route to keep network balanced.

3.1 System Model & Location Based Cluster Formation

The theoretical model for proposed model implementation is shown in Fig. 1. Nodes are randomly distributed in sensor region based on random way point mobility model. The MCH is located in constant position whereas DCH is located with some mobility. The nodes are categorized into various groups of clusters and cluster count determines number of clusters in the region. The intra and inter cluster communication are permitted as per the cluster norms.

In this phase, cluster region is constructed with equal size and cluster members and communication through multi-hop communication. Here the cluster is formed with 5 cluster heads and randomly deployed cluster members. Based on geographical location of nodes and reliability of paths, cluster is formed to increase the energy efficiency. It is observed from existing works, the network zone is divided into discrete and unbalanced regions which results in more energy consumption and less network lifespan. Initially the source node discovers the route to sink node by flooding packets i.e. *R_DS* to neighbour nodes. These packets contain the formation of cluster through reliable routes. After receiving the *R_DS* packets by neighbour nodes, *R_REP* will be sent to source node to join the route for packet forwarding. Each node chooses its neighbour node based on least hop count path and updates their routing tables. If the construction of routing table is finished, next hop will be identified and the location co-ordinates will be broadcast. The nodes which are located in the coverage area, MCH determines center location metric based on location co-ordinates. Nodes are located near to center location metric to form high energy efficient clusters with least overhead. Based on location based clustering, it is easy to reduce the computational cost through optimum cluster head election mechanism. The selection of CH is based on stability, reliability, data confidentiality and residual energy factor. The cluster is formed based on one of the factors called optimum energy node metric (E_{OT}) to balance energy consumption based on energy factor which is given as: $E_{OT} = \mu \times e_{\text{node}}$, where μ is the ratio of reduced energy of node to total energy and e_{node} is the total energy of node. Node hub $H(x)$ is defined to choose initial MCH and DCH that needs least control overhead and less energy consumption. Node hub is derived as

$$H(x) = \frac{1}{\sum_{k=1}^{m} d(a, b_k)} \tag{1}$$

where m is the node and $d(a, b_k)$ is the distance from location from a to b while node is moving from one position to another position. Fig. 1 shows the illustration of cluster formation through the location of nodes.

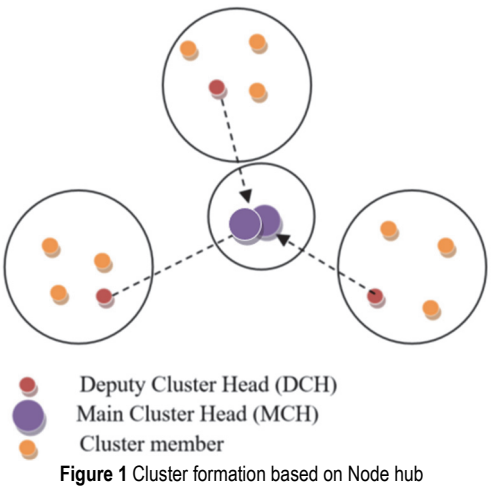

Figure 1 Cluster formation based on Node hub

3.2 Optimal Multicast Route Discovery for Packet Forwarding

In this phase, packets are routed towards destination via multiple paths. By obtaining reliability of path, it is easy to forward packets which will produce data confidentiality and least packet loss. The steps are provided to identify reliable route among multiple paths.

In this phase, reliable route among multicast routes is chosen from MCH to DCH and DCH to Cluster Members (CMs). Let us consider that MCH sends the packets to DCH and DCH forwards to CMs. Assume that M disjoint routes are found from MCH to DCH and DCH to Cluster Members (CMs). Each path p_k, $k = 1,2,....X$ contains neighbour nodes $m_{kl}\left(1,2,.....M\right)$. The corresponding residual energy is denoted as ε_{kl} with $0 \le \varepsilon_{kl} \le 1$. The energy consumed on path p_k is E_k the lowest energy for forming the optimal path i.e. $E_k = \min\left(\varepsilon_{kl}\right)$. The optimal path is obtained based on energy consumption of link $\left(E_k\right)$ and packet transmission period $\left(\tau_a\right)$. The maximum-minimum required energy (for route m) based routing is chosen to identify optimal path with maximum link energy $\left(E_k\right)$ and high packet transmission period $\left(\tau_a\right)$ and it is denoted as:

$$m = \arg\max_{1 \le k \le M}\left\{\min_{1 \le k \le M}\left(\varepsilon_{kl}\right)\right\} \tag{2}$$

The path with maximum-minimum required energy is preferred as optimal multicast. The link energy consumption $\left(E_k\right)$ is given as:

$$E_k = \tau_a\left(P_c + P_{t,k}\right) + T_t P_t \tag{3}$$

whereas P_c, $P_{t,k}$, T_t and P_t are the power consumption of cluster region, transmitting power with respect to time t from node k, transmitting period and transmitting power originated from one cluster region to all others.

Delay $\left(d_{(MCH,DCH,CMs)}\right)$ is also taken into consideration for determining the optimal path from MCH to DCH and DCH to CMs. The path with less delay is considered as optimal path for forwarding packets to sink node.

$$d_{(MCH,DCH,CMs)} = \frac{\max\limits_{\tau=1}^{N_{MCH}^{DCH}}\left(N_{DCH}^{CMs}\right)}{d} \tag{4}$$

where d indicates that number of clusters present in the region which are located and connected through stable paths and N_{MCH}^{DCH} implies that Deputy Cluster Head (DCH).

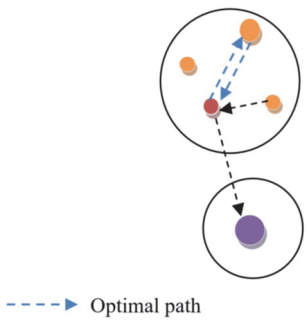

Figure 2 Selection of optimal multicast route

Fig. 2 presents the selection of optimal path in the cluster region. In this phase, optimal multicast routes are maintained with least hop count and low cost value. Both MCH and DCH record the status of optimal routes and choose the route for packet transmission. At the end of process, the routes are kept idle.

3.3 Energy Model

In the cluster network, energy is a major concern during data transmission. Both MCH and DCH keep high residual energy at the end of data transmission process. Because it records the routing history in routing table and deletes periodically once them optimal route expires. It consumes less energy for packet transmission. Either MCH or DCH keeps the residual energy $\left(E_{\text{residual}}\right)$ at maximum level and the difference is estimated between energy consumed on current packet transmission $\left(E_{\text{current}}\right)$ and previous packet transmission $\left(E_{\text{prev}}\right)$ and it is derived as:

$$E_{\text{residual}} = E_{\text{current}} - E_{\text{prev}} \tag{5}$$

The energy consumed by MCH for transmitting packet to DCH during intracluster transmission is given as:

$$E_{MCH\ \text{to}\ DCH} = \sum_{e=1}^{M}\sum_{a=1}^{v} E_n\left(M, MCH_a\right) \tag{6}$$

where v is the number of cluster members and $E_n\left(M, MCH_a\right)$ is the amount of energy spent from MCH to DCH. The energy consumed by DCH for sending packet to cluster members is the sum of energy consumed in data aggregation $\left(E_{\text{nag}}\right)$, energy consumed for packet reception from DCH to CMs $\left(E_{\text{nrec}}\right)$. The energy is calculated as:

$$E_{DCH\ \text{to}\ CM} = E_{\text{nag}} + E_{\text{nrec}} \tag{7}$$

The total energy of cluster region is the sum of energy spent by MCH, DCH and CMs and it is the energy metric to choose the optimal route.

3.4 Election of MCH and DCH

In this phase, MCH is chosen based on residual energy and stability index. The voting scheme is initialized to select the MCH and DCH. Cluster members are requested to vote for choosing CHs. The following query parameters are used to select the Optimal MCH and DCH.

1. Distance to cluster center
2. Residual energy factor
3. Stability index

Distance to cluster center

For nodes $\left(y,z\right)$, the distance between their geographical location and DCH is calculated as:

$$d = \sqrt{\left(y_{\text{node}} - y_{MCH}\right)^2 + \left(z_{\text{node}} - z_{MCH}\right)^2} \tag{8}$$

The node which is nearer to DCH has high residual energy. The node has more than 80% residual energy, can be nominated for CH.

Residual energy factor

Residual energy factor $\left(R_{EF}\right)$ is one of the major parameters to choose CH. Here the factor is estimated as remaining energy after the data transmission process.

$$R_{EF} = E_r - E_{tot} \tag{9}$$

The node which is maintaining more than 95% remaining energy can be nominated for CH.

Stability Index (SI)

Stability index is determined from Packet Delivery Ratio (PDR) and capacity of node (*c*). If the two factors are good, stability index of node SI_n will also be good.

$$SI_n = PDR \times \left(1 - e^c\right)$$

Packet delivery ratio is defined as the ratio of packet arrived at sink node to total number of packets sent successfully from source node. The node capacity means to carry and store the packets in the predefined level. Based on the parameter SI is estimated and lies from 0.8 to 1.0 with respect to received signal strength. The optimal MCH and DCH is chosen based on above mentioned parameters to ensure effective packet arrival and reliability in the cluster region.

3.5 Reliable Model for Secure Packet Forwarding

In this phase, direct and indirect reliability index of cluster region is estimated to secure data transmission from MCH to DCH and DCH to CMs. If any node falls below the reliability index, it will be detected and isolated from the cluster group immediately. The direct reliability index $\left(DRI_0^N\right)$ is used to represent the reliability between MCH and DCH, DCH and CMs. It means that the reliability of nodes is maintained for secure packet transmission in inter and intra cluster communication region. The direct reliability index is the ratio of number of reliable packets successfully transmitted and omitting the duplicate packets to the total number of packets available for transmission. The duplicate packets are identified using packet index and dropped by the neighbour node based on the instructions received from DCH and MCH. The direct reliability index is estimated as:

$$\begin{aligned} DRI_0^N &= \frac{P_r - P_d}{P_t} \\ DRI_0^N\left(MCH, DCH\right) &= A_0^N\left(MCH, DCH\right) \\ DRI_0^N\left(DCH, CMs\right) &= A_0^N\left(DCH, CMs\right) \end{aligned} \tag{10}$$

where *A* indicates that authenticated packet transmission between nodes.

The indirect reliability index $\left(IRI_0^N\right)$ between MCH and DCH, DCH and CMs is estimated based on feedback about the sensor nodes. To achieve secure data communication, node requests feedback of other nodes about the routing history, packet transmission capability, stability index, residual energy factor. The DCH gathers feedback of other nodes for estimating indirect reliability index based on following representation,

$$IRI_0^N = F\left(R_h, P_{tc}, SI_n, R_{EF}\right) \tag{11}$$

where *F* indicates that feedback which is a function of above said parameters of sensor nodes. The total reliability index is the sum of direct and indirect reliability index to provide security for data transmission, and balance the security and energy to prolong the network lifespan.

3.6 Fuzzy Decision Model

Fuzzy decision is one of major parts in fuzzy theory mechanism. Decision is taken based on parameters and rules taken on the system. In the decision model, results are taken as composite events which are used to identify the event which is under the system rules. The attribute set of calculating solution is $RE = \left\{re_1, re_2, ...re_n\right\}$ and the decision model set is $A = \left\{A_1, A_2, ...A_m\right\}$, decision model elements are ordered, *RE* is the residual energy and *A* is the authentication factor. The following steps are used to balance the energy and security based on fuzzy decision.

Step 1: The degree matrix of membership function of attribute is denoted as $K = V_{ab}\left(x\right)_{m \times n}$ and it is represented as:

$$K = \begin{pmatrix} v_{1x}(x) & v_2(x) & .... & v_{1n}(x) \\ v_{1x}(x) & v_{1x}(x) & ... & v_{1x}(x) \\ .... & ... & .... & ... \\ v_{1x}(x) & v_{1x}(x) & ... & v_{1x}(x) \end{pmatrix}$$

Step 2: Input values to Fuzzification module are Residual energy factor and reliability index.

Step 3: Decision matrix is derived as,

$DM = \left(re_{ab}, RI\right)_{n \times m}$, where $re_{ab} = w_b \times K$ and $RI = z_b \times K$ where w, z are the weight factors of attribute matrix.

Step 4: Crisp values are processed in the fuzzy inference system.

Step 5: The balanced index is decided at defuzzification module.

Step 6: If both *re* and *RI* are high, the balanced index will be one or else zero. If one, it means the system is good and withstands any attacks consuming least energy. If zero, it means the system is not balanced in both security and energy in the network.

3.7 Proposed Packet Format

Fig. 3 shows the proposed packet format. The first three fields of the packet contain id of DCH, MCH and CM that occupies 2 bytes. Fourth and fifth field occupied 2 bytes by residual energy of node and balanced index of cluster region and the last field contains frame check

sequence used for error checking and correcting in the frame during transmission.

MCH ID	DCH ID	CM ID	Residual energy	Balanced Index	FCS
2	2	2	2	4	4

Figure 3 Proposed packet format

Fig. 4 shows the illustration of proposed routing mechanism for achieving balancing between network security and energy level.

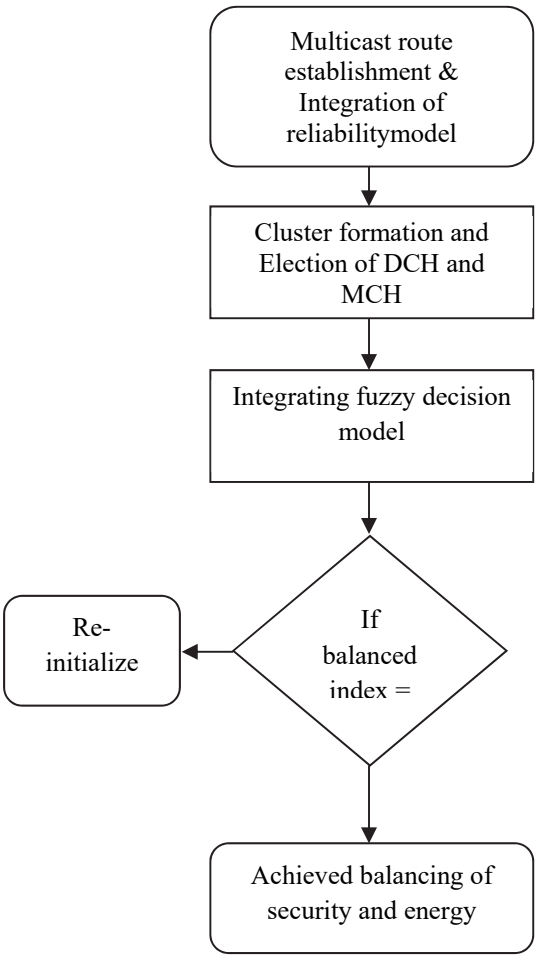

Figure 4 Flow of proposed routing mechanism

4 SIMULATION SETUP

Network Simulator Tool (NS2.35) is used for simulation of proposed protocol in terms of network parameters. Tab. 1 shows simulation settings of proposed protocol.

Table 1 Simulation settings

Cluster count	5
Number of Sensor nodes	1000
Simulation area	1000 x 1000 sq.m.
Mobility model	Random Way Point
Traffic	Constant Bit Rate (CBR)
Routing Protocol	LEACH
Packet rate	5 packets/sec

4.1 Peformance Metrics

Location accuracy rate: It is the rate at which geographical position of node is with respect to center hub.

Packet delivery ratio: It is the ratio of packets arrived at sink node to packets sent.

Control Overhead: It means that additional resources are required to transmit and receive the packets.

End to end delay: Delay consumed for packet transmission from MCH to DCH and DCH to CMs.

Route reliability ratio: It is the ratio of detection of optimal route to total number of routes.

Residual energy rate: It is the rate at which node has remaining energy after entire data transmission.

The following protocols and schemes like CEEA [9], PDKM [10], and TEMOHOA [16] are compared with proposed protocol QLAMSR.

Tab. 2 shows the comparative analysis of Proposed and Existing schemes with data taken from simulation analysis.

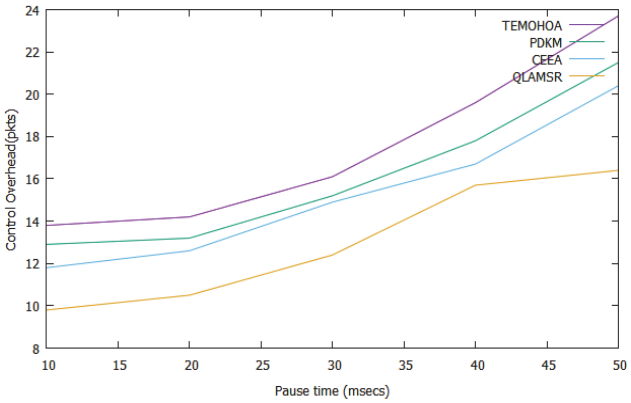

Figure 5 Control overhead vs pause time

Fig. 5 shows that proposed protocol consumes less overhead (9.8-16.4) packets for excessive packet transmission than existing schemes because of integration of optimal multi-cast route discovery process.

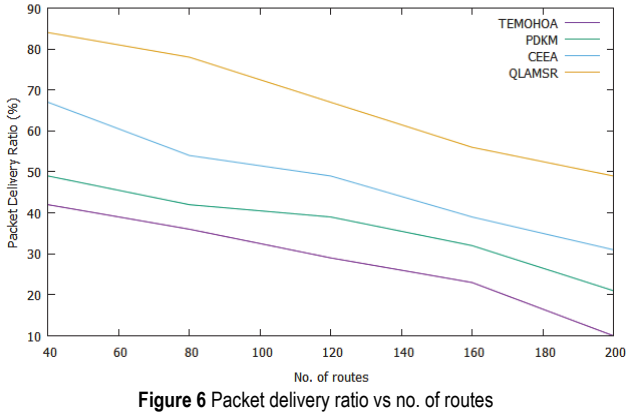

Figure 6 Packet delivery ratio vs no. of routes

Fig. 6 implies that proposed protocol achieves higher packet delivery ratio (84-49)% than existing schemes due to the presence of effective cluster heads.

Fig. 7 presents the comparison of location accuracy rate (42-239) nodes/ degree of proposed and existing schemes. The proposed protocol achieves high accuracy because of integration of location co-ordinate system.

Fig. 8 provides the performance of route reliability ratio (17-189). The proposed protocol contains more reliable routes due to integration of optimal route selection and reliability index.

Fig. 9 shows the results of end to end delay (3.8-10.8) msecs. It is seen that proposed protocol consumes less delay because of selection of CH and node reliability.

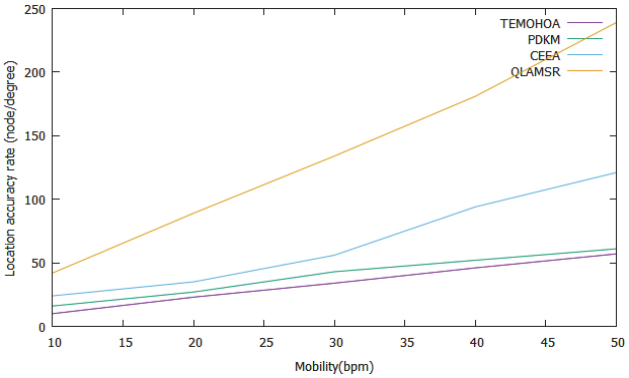

Figure 7 Location accuracy rate vs mobility

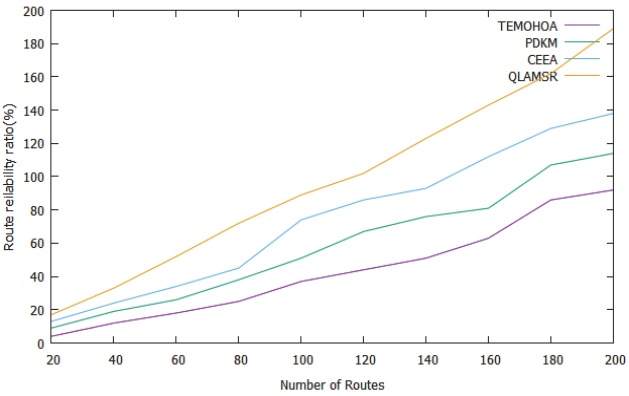

Figure 8 Route reliability ratio vs number of routes

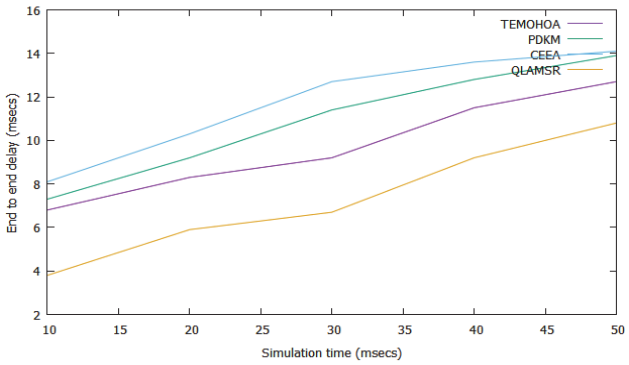

Figure 9 End to end delay vs simulation time

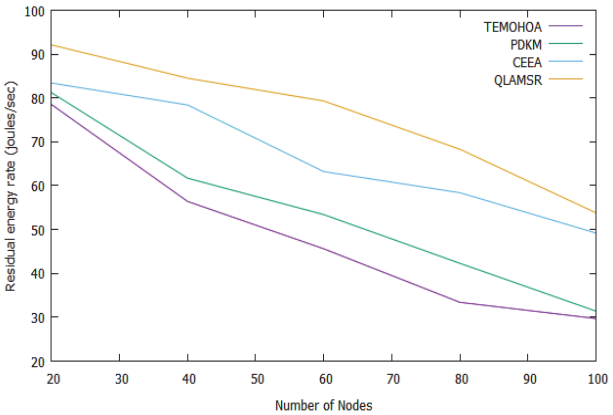

Figure 10 Residual energy rate vs number of nodes

Fig. 10 shows the comparison of residual energy (92.1-53.8) joules/sec for proposed and existing schemes. It seems that while varying the number of nodes, residual energy of proposed protocol achieves higher energy than existing schemes because of the energy model and maintaining constant bit rate of traffic during packet transmission. Tab. 2 shows the comparative results of proposed and existing schemes.

Table 2 Comparative results

Performance Metrics	QLAMSR	TEMOHOA	PDKM	CEEA
Residual energy rate / joules/sec	92.1-53.8	78.5-29.7	81.2-31.4	83.4-49.2
Control Overhead / pkts	9.8-16.4	13.8-23.7	12.9-21.5	11.8-20.4
End to end delay / msec	3.8-10.8	6.8-12.7	7.3-13.9	8.1-14.1
Route reliability ratio / %	17-189	4-92	9-114	13-138
Packet delivery ratio / %	84-49	42-10	49-21	67-31
Location accuracy rate / nodes/degree	42-239	10-57	16-61	24-121

5 CONCLUSION

Energy and Security is an indivisible part in sensor network. The research work was focused on balancing energy and security. Using location aided cluster formation, efficient CHs are nominated to forward the packets through optimal multicast routes. MCH and DCH are the key nodes for tracking and updating the route and packet transmission status. Reliability model is implemented for securing packets from the attackers. Here the reliability index is used for identifying the reliable nodes. Energy model is introduced for increasing residual energy. Fuzzy decision model is integrated to provide assistance for ensuring scalable and efficient network. The proposed protocol is simulated and performs better than existing schemes with various performance metrics like residual energy rate, control overhead, end to end delay, route reliability ratio, location accuracy rate and packet delivery ratio. In future work, polynomial cryptosystem and symmetric key approaches will be implemented for focus on security challenges of WSN.

6 REFERENCES

[1] Lim, S. (2021). A Chain-Based Wireless Sensor Network Model Using the Douglas-Peucker Algorithm in the Iot Environment. *Tehnicki vjesnik-Technical Gazette*, *28*(6), 1825-1832. https://doi.org/10.17559/TV-20200916075229

[2] Chen, W., Liu, Y., Liu, C., Ma, H., & Wu, H. (2021). An Invulnerability Algorithm for Wireless Sensor Network's Topology Based on Distance and Energy. *Tehnicki vjesnik-Technical Gazette*, *28*(6), 2147-2155. https://doi.org/10.17559/TV-20201130023106

[3] Asaad, A, Baidaa, K., & Imad, A. (2022). Fuzzy Data Aggregation Approach to Enhance Energy-Efficient Routing Protocol for HWSNs. *Informatica*, *46*, 47-54. https://doi.org/10.31449/inf.v46i7.4272

[4] Deniz, T., Cem, T., & Selçuk, Y. (2021). Container-Based Virtualization for Bluetooth Low Energy Sensor Devices in Internet of Things Applications. *Technical Gazette*, *28*(3), 13-19. https://doi.org/10.17559/TV-20180528134139

[5] Qureshi, K. N., Bashir, M. U., Lloret, J., & Leon, A. (2020).

Optimized Cluster-Based Dynamic Energy-Aware Routing Protocol for Wireless Sensor Networks in Agriculture Precision. *Journal of Sensors*, *2020*, 1-19. https://doi.org/10.1155/2020/9040395

[6] Abhishek, J., Vishal, J., & Khushboo, T. (2020). Trust based Intrusion Detection System Architecture for WSN. *International Journal of Recent Technology and Engineering*, *8*(6), 700-703. https://doi.org/10.35940/ijrte.F7329.038620

[7] Girish, D., Abdull, R., & Niranjan, S. (2018). Energy Efficient and Secure Routing Technique for Wireless Sensor Networks. *International Journal of Current Advanced Research*, *7*(2), 10309-10314. https://doi.org/10.24327/ijcar.2018.10314.1740

[8] Xiuniao, Z., Wentao, Z., & Yahya, N. (2022). A Novel Energy-Aware Routing in Wireless Sensor Network Using Clustering Based on Combination of Multi-objective Genetic and Cuckoo Search Algorithm. *Wireless Communications and Mobile Computing*, *2*(1), 1-14. https://doi.org/10.1155/2022/6939868

[9] Jie, C., Prasanna, D., Nicholas, C., Mohammed, A., & Cormac, S. (2022). Controller-Based Energy-Aware Wireless Sensor Network Routing Using Quantum Algorithms. *IEEE Transactions on Quantum Computing*, *3*(1), 1-12. https://doi.org/10.1109/TQE.2022.3217297

[10] Eid, R., Muhammad, S., Syed, N., & Anwar, G. (2020). Polynomial Based Dynamic Key Management for Secure Cluster Communication in Wireless Mobile Sensor Network. *Technical Gazette*, *27*(2), 358-367. https://doi.org/10.17559/TV-20170807075015

[11] Meysam, Z. & Mohammadreza, S. (2020). A Gray System Theory Based Multi-Path Routing Method for Improving Network Lifetime in Internet of Things Systems. *Preprints,* 1-28. https://doi.org/10.20944/preprints202001.0304.v1

[12] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Khannah Nehemiah, H., & Kannan, A. (2019). An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks. *Wireless Personal Communications*, *105*, 1475-1490. https://doi.org/10.1007/s11277-019-06155-x

[13] Gopinath, S., Vinoth Kumar, K., Elayaraja, P., Parameswari, A., Balakrishnan, S., & Thiruppathi, M. (2022). SCEER: Secure Cluster Based Efficient Energy Routing Scheme for wireless sensor networks. *Material today proceedings*, *45*, 3579-3584. https://doi.org/10.1016/j.matpr.2020.12.1096

[14] Manjunath, H. & Guruprakash, D. (2022). Energy-Efficient Routing Protocol for Hybrid Wireless Sensor Networks using Falcon Optimization Algorithm. *International Journal of Intelligent Engineering and Systems*, *15*(4), 1-10. https://doi.org/10.22266/ijies2022.0831.01

[15] Eswaramoorthy, V., Vinoth Kumar, K., & Gopinath, S. (2021). Fuzzy logic based DSR trust estimation routing protocol for MANET using evolutionary algorithms. *Technical Gazette*, *28*(6), 2006-2014. https://doi.org/10.17559/TV-20200612102818

[16] Kantharaju, V. & Sanjeev, L., (2022). Trust and Energy Based Multi- Objective Hybrid Optimization Algorithm for Wireless Sensor Network. *International Journal of Intelligent Engineering and Systems*, *15*(5), 71-80. https://doi.org/10.22266/ijies2022.1031.07

[17] Wang, X., Liu, X., Wang, M., Nie, Y., & Bian, Y. (2019). Energy-Efficient Spatial Query-Centric Geographic Routing Protocol in Wireless Sensor Networks. *Sensors*, *19*(10), 2363-69. https://doi.org/10.3390/s19102363

[18] Kavana, E. (2022). Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *10*(8), 4221-4231. https://doi.org/10.22214/ijraset.2022.45959

[19] Banerjee, A. & Ghosh, S. (2019). Weight-based Energy-efficient Multicasting (WEEM) in Mobile Ad-Hoc Networks. *Procedia Computer Science*, *152*, 291-300. https://doi.org/10.1016/j.procs.2019.05.014

[20] Arzoo, M., Tarunpreet, B., Gaurav, S., & Gulshan, S. (2017). An Energy Efficient and Trust Aware Framework for Secure Routing in LEACH for Wireless Sensor Networks. *Scalable Computing: Practice and Experience*, *18*(3), 207-218. https://doi.org/10.12694/scpe.v18i3.1301

[21] Saini, A., Kansal, A., & Randhawa, N. S. (2019). Minimization of Consumption in WSN using Hybrid WECRA Approach. *Procedia Computer Science*, *155*, 803-808. https://doi.org/10.1016/j.procs.2019.08.118

[22] Vinoth Kumar, K., Jayasankar, T., Eswaramoorthy, V., & Nivedhitha, V. (2020). SDARP: Security based Data Aware Routing Protocol for Ad hoc Sensor Networks. *International Journal of Intelligent Networks*, *1*(2020), 36-42. https://doi.org/10.1016/j.ijin.2020.05.005

Contact information:

Mr. Karthick CHANDRASEKARAN, Assistant Professor
(Corresponding author)
Department of Electronics and Communication Engineering,
Dhaanish Ahmed Institute of Technology,
Coimbatore - 641105
Email: karthickecephd@gmail.com

Dr. Kathirvel CHINNASAMY, Professor
Department of Electrical and Electronics Engineering,
Sri Ramakrishna Engineering College,
Coimbatore - 641029