EAI Endorsed Transactions
on Energy Web

Research Article EAI.EU

A Markov Process-based Opportunistic Trust Factor Estimation Mechanism for Efficient Cluster Head Selection and Extending the Lifetime of Wireless Sensor Networks

Sengathir Janakiraman[1], M. Deva Priya[2,*], S. Siamala Devi[2], G. Sandhya[2], G. Nivedhitha[2], S. Padmavathi[2]

[1]Department of Information Technology, CVR College of Engineering, Mangalpally, Vastunagar, Hyderabad, Telangana, India
[2]Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, Tamilnadu, India

Abstract

INTRODUCTION: The lifetime of a sensor network completely relies on the potentialities of the utilized Cluster Head (CH) selection scheme that aids in building efficient Wireless Sensor Networks (WSNs). Most of the existing CH selection approaches use an impractical condition which mainly emphasizes that the nodes that are trustworthy and highly energy competitive have better likelihood of being selected as CHs.

OBJECTIVES: In this paper, a Markov Process-based Opportunistic Trust Factor Estimation Mechanism (MPOTFEM) is proposed for achieving optimal CH selection that enhances the possibility of maintaining network lifetime and energy stability in the network.

METHODS: MPOTFEM is proposed for ensuring efficient CH selection and thereby enhancing the lifetime of WSNs. The proposed MPOTFEM incorporates the merits of Markov process for computing the Opportunistic and Trust factors that assesses the maximum likelihood of nodes with the possibility of being selected as the CH by exploring multiple transition states of nodes in the networks.

RESULTS: The results of the propounded MPOTFEM confirm to be significant in improving the network longevity by

analysis.

CONCLUSION: The results prove that MPOTFEM is better when compared to the benchmarked CH selection schemes in terms of network lifespan and energy stability

Keywords: Markov Process, Opportunistic Factor, Trust Factor, Cluster Head Selection, Network Lifetime, Maximum Likelihood Probability

Received on 26 October 2020, accepted on 23 December 2020, published on 13 January 2021

doi: 10.4108/eai.13-1-2021.168093

*Corresponding author. Email: M.devapriya@skct.edu.in

1. Introduction

Wireless Sensor Networks (WSNs) are suitable for potential applications used in monitoring real-time environments including military operations, weather forecasting, health monitoring and network surveillance (Rajarajeswari et al 2015). This WSNs involve hundreds and thousands of sensor nodes for achieving sensing and data aggregation operation (Janakiraman 2018).

However, the limited energy and memory, computation time and ability of sensor nodes introduce crucial issues that have a negative influence on the performance of the network. Further, the lifespan of the network is purely based on the amount of resources available and adoption

of suitable clustering algorithms (Rambabu et al 2019a). In this context, the clustering process which organizes closely located sensor nodes into groups called clusters are determined to be suitable for achieving effective and efficient management of clusters. However, the significance of the clustering algorithms is based on the incorporated Cluster Head (CH) selection process (Rambabu et al 2019b). Further, the clustering schemes should be capable of balancing energy of nodes in the network. More number of clustering algorithms are available in the literature using random or probabilistic CH election mechanisms to mainly focus on the energy balance which in turn improves network lifetime (Priya et al 2020; Janakiraman & Priya 2020). At this juncture, the problem definition is presented as follows: Given a set of sensor nodes deployed in the network with predefined energy levels, then the problem is to focus on the selection of CH nodes that aid in the clustering process wherein multiple clusters are formed with maximized energy level and optimized inter and intra-cluster distance between them.

In this paper, a Markov Process-based Opportunistic Trust Factor Estimation Mechanism (MPOTFEM) is propounded for efficient CH selection in WSNs so as to offer enhanced lifetime of the network. The consecutive steps in the implementation of the propounded MPOTFEM technique with the necessary algorithm and flowchart are presented. It shows the simulation and the results of the implementation of the proposed mechanism for varying number of sensors.

2. Related Work

Clustering supports shaping a network into a linked hierarchy, enabling load balancing and extending the lifespan of a network. Fuzzy logic supports wise combinations of diverse parameters. Taheri et al (2012) have propounded an Energy-aware distributed dynamic Clustering Protocol (ECPF) which is based on the following factors namely, non-probabilistic CH selection, use of fuzzy logic and on-demand clustering. The Residual Energies (REs) of nodes are taken as the chief parameters for selecting CHs non-probabilistically based on the delay that is inversely proportional to the RE of a node. CHs are chosen based on their RE, and fuzzy logic is used to assess a node's appropriateness in being elected as a CH from adjacent CHs. Other nodes link to the CH with minimum fuzzy cost.

Nodes in the Region of Interest (RoI) send sensed data to the BS and it always fulfils the frequency of data collection demanded by the BS. Wang & Chen (2012) have propounded a link-aware clustering scheme called Link-aware Clustering Mechanism (LCM) to find an energy-proficient and trusted path. It chiefly takes the node and link status and uses a clustering parameter, Predicted Transmission count (PTX) to assess the requirement of nodes of CHs and Gateways (GWs) to form clusters. Each CH or GW is based on the PTX to find the priority, and the candidate with the maximum priority is elected as the CH and GW.

Clustering prolongs the lifespan of a sensor network by minimizing energy depletion. It extends network lifespan and enhances scalability. Wang et al (2013) have propounded Hybrid Distributed Energy-Efficient Heterogeneous Clustered (HDEEHC) protocol for WSN. This protocol occasionally chooses CHs based on the hybrid of primary and secondary parameters. The RE and node type are the parameters involved in the CH, along with the immediacy to its adjacent nodes or node degree. The nodes with more preliminary RE are more likely to be chosen as CHs than the nodes with lesser energy.

Dynamic clustering supports scalability and energy efficient data accumulation in WSN. Nevertheless, it is prone to unfair energy consumption in inter-cluster communication. Xu et al (2015) have proposed Distributed and Adaptive Routing protocol for Cluster-based wireless sensor networks (DARC) wherein, a dynamic energy threshold is determined for CH to deal with the inter-cluster routing approach, and a cost function is found for relay choice. DARC deals with balancing energy consumption for inter-cluster communication and increases energy proficiency and network lifetime.

Thilagavathi & Gnanasambandan Geetha (2015) have propounded an enhanced binary Particle Swarm Optimization (PSO) algorithm with altered Connected Dominating Set (CDS) based on RE for finding the optimum number of clusters and CHs. This mechanism is propounded with the benefits of maximum likelihood probability in order to determine the correlation between their behaviors.

Zhou et al (2016) have propounded a CH selection scheme for dealing with the challenges introduced by insider selective forwarding attack. This mitigating scheme uses specifically chosen nodes like inspector and cluster member for avoiding the damage of the whole network. This CH election mechanism involves composite reputation by estimating excess energy and forwarding rate of nodes. The lifetime of the network and false alarm rate of the propounded scheme are minimized. The inspector observes the transmissions to defend the cluster and the CH transmits packets from members and other CHs, and arbitrarily observes the inspector nodes to determine whether they are working properly. The normal nodes in addition to forwarding data, observe the behaviors of the CH and inspector nodes using a reputation scheme.

Wang et al (2016) have proposed a combined energy and trust based CH election mechanism for enhancing the network lifetime. This scheme deals with the scalability by implementing a hierarchical architecture that stabilizes organization of lower and higher end sensors. The CHs are fortified with a Trusted hardware Module (TM). To ensure energy efficiency in a network, a Trusted hardware based Energy Efficient Clustering (TEEC) mechanism is propounded to choose suitable CHs. The lifetime of this approach is extended and promises protection against

replay attacks, provides node authentication and information privacy for fighting against the compromise of sensors. Nevertheless, the amount of dead and alive nodes evaluated for varying number of sensor is same as the traditional probabilistic CH election schemes.

Conventional cryptography schemes are not appropriate for WSNs as they have their own power and resource restraints. Managing trust assists in enhancing security and handling threats in WSNs. Trust is the degree of trustworthiness in a node. Low Energy Adaptive Clustering (LEACH), a cluster based routing scheme is better when compared to direct communication protocols but has some security flaws. Miglani et al (2017) have proposed an Energy Efficient and Trust Aware in LEACH (EETA-LEACH) for secured routing. This scheme is an amalgamation of trust-based routing and management for efficient selection of CH.

The durability of a sensor network depends on the efficiency of CH selection that features towards operative management in WSNs. The CHs that are highly energy efficient and trusted are elected as CHs. Amuthan & Arulmurugan (2018) have propounded an Availability Predictive Trust Factor-based Semi-Markov Mechanism (APTFSMM) for efficient CH election so as to enhance its durability in WSNs. The proposed mechanism inherits the advantages of semi-Markov process for assessing the availability prognostic trust factor that enumerates the maximum probability based on which a node can be elected as the CH through increased exploration of several transition states of nodes. A mechanism that focuses on designing energy efficient CH selection considers that the partaking nodes are reliable, while the trust-based CH election schemes consider that nodes are energy efficient. These expectations are not convincing as the historical or present RE of nodes may not assist in determining an optimal CH. Amuthan & Arulmurugan (2018) have presented an integrated energy and trust based prediction scheme called Hyper-Exponential Reliability Factor-based Cluster Head Election (HRFCHE) that is based on Semi-Markovian approach for extending network lifetime.

Mythili et al (2019) have proposed Spatial and Energy Aware Trusted Dynamic Distance Source Routing (SEAT-DSR) algorithm for improving the lifetime of WSNs. The spatial data, RE and data quality are balanced by the energy aware routing algorithms based on Quality of Service (QoS). Further, a clustering algorithm is also included for forming a group of sensors based on the aforementioned parameters along with the trust score and inter-node distance. The scheme makes decisions and a hierarchical trust scheme is presented which is based on network size, energy involved, speed of communication and recommendation. It focuses on the enhanced sliding window time by assuming the presence of attackers to find their inconsistent behavior. Rodrigues & John (2020) have proposed a routing algorithm based on trust for secured routing. Chicken Dragonfly (CHicDra) optimization algorithm is also proposed for supporting trusted communication by finding optimal CHs in the network. Once CHs are chosen with multi-objective Taylor Crow Optimization (TCO), the reliable nodes are confirmed using joint trust that is based on the trust factors that include integrity, consistency, forwarding rate and availability. CHicDra is a variation of the Chicken Swarm Optimization (CSO) with dragonfly algorithm. Lastly, a secure and reliable path is chosen for communication. Sharma et al (2020) have proposed reliable and energy based clustering scheme called energy efficient Trusted Moth Flame Optimization and Genetic Algorithm (eeTMFO/GA). The CHs are selected using MFO in a clustered network. The fitness function is based on parameters like packet forwarding progress, RE, connected node density, mean cluster distance and mean transmission delay.

3. Proposed Markov Process-based Opportunistic Trust Factor Estimation Mechanism (MPOTFEM)

The proposed Markov Process-based Opportunistic Trust Factor Estimation Mechanism (MPOTFEM) incorporates the merits of determining the Opportunistic factor of nodes by merging their up and down times for attaining better CH selection. The Failure (F) and Preventive Maintenance (PM) states of nodes are considered for enumerating their availability in co-operative data distribution in the network. The proposed mechanism is found to be exceedingly trustworthy for CH selection as it securely chooses CHs by identifying the malevolent features of nodes. It is predominant to focus on effective CH selection so as to minimalize the frequency in change of roles of selected CH nodes in the network. It also focuses on the construction of an energy competent CH selection technique that wholly targets in maximizing the network lifetime.

The proposed MPOTFEM is an effectual clustering algorithm that aims at efficient choice of CH by predicting the Opportunistic factor of nodes. The proposed MPOTFEM determines this factor as it is an unusual instance of trustworthiness. Availability is analyzed based on the node's resilience during CH selection. Resilience factor is involved as the nodes are expected to be rehabilitative in nature. In particular, the Resilience factor shows significant accessibility rate of nodes with well-defined utilization conditions. The nodes' Opportunistic factors need to be possibly reclaimed at any point of time independent of the risks encountered in the process, thus facilitating indispensable functionalities in the network. Moreover, the opportunistic nature of a node refers to the intrinsic competence of nodes to convert its trustworthiness and resilience into an assessment index that contributes to network performance.

In the proposed MPOTFEM, the nodes are found to be transformed from their failure state. The proposed MPOTFEM takes into consideration the functioning and preventive resilience time of nodes into account. It also takes the operating and failure times of nodes for enumerating their accessibility in the network. The steps

of the propounded MPOTFEM comprises of the following: i) Measuring the nodes' Maximum Likelihood Transition Probability ii) Estimation of transition function values related to complete states of node and iii) Computation of Markov Availability Prediction Trust Factor (MAPTF).

3.1 Estimation of a nodes' Maximum Likelihood Transition Probability

The Maximum Likelihood Transition Probability (MATP) of nodes is found based on the trust and energy values extracted from the network by including probe packets in the control packets utilized for data communication. MATP is computed for enumerating the probability of nodes during their shift between states [109]. The energy model employed in the propounded MPOTFEM is same as the energy model in the proposed HGRF-OCHP technique. Furthermore, MATP is computed based on direct and indirect interactions among nodes. The maximum transition probability of nodes defined in the propounded MPOTFEM is shown in Table 1.

Table 1: Nomenclature

Symbol	Explanation
$\varphi_{C\_E}^{S}$	Probability of a cooperative node converted into a selfish node to conserve energy
$\varphi_{S\_E}^{F}$	Probability of a selfish node moving to the failed state as its RE falls below the used energy threshold factor
φ_{O}^{C}	Probability of an operating selfish node entering into cooperative state when the energy of a node is enhanced
φ_{N}^{C}	Probability of a non-cooperative selfish node getting transformed into a cooperative node by using appropriate energy refining schemes
φ_{S_E}	Probability of a selfish node to remain in its state due to its inability to improve energy level
$\varphi_{C}^{S,F}$	Node in cooperative state with probability of getting converted to selfish or failed state
$\varphi_{S}^{F,O}$	Node in selfish state with a probability of entering into failed state or regaining its state
φ_{S}^{C}	Node in selfish state with a probability of returning to its cooperative state
φ_{S}	Node in selfish state with a probability of prevailing in the same state
φ_{S}^{F}	Node in selfish state with a probability of moving to failed state
$\varphi_{F\_E}^{C,S}$	Node in failed state with a probability of being reformed into selfish or cooperative state depending on the quantity of available energy
φ_{PM}^{O}	Probability with which the state of a node is transformed into its operating state
φ_{O_PM}	Probability with which a node exhibits comprehensive operating behaviour
$\varphi_{F\_PM}^{S}$	Probability with which a node enters into failed state in spite of using preventive maintenance approach
μ_{NO}^{O}	Mean rate of transforming a non-operating node into an operating node
φ_{MPOTF}	Markov Process-based Opportunistic Trust Factor
μ_{MPOTF_PM}	Mean rate of a node transformed from failed to operating state in spite of using Preventive Maintenance (PM) approach
$\varphi_{O\_PM}^{C}$	Probability of an operating selfish node entering into cooperative state in spite of using Preventive Maintenance (PM) approach
$\varphi_{F\_E}^{S}$	Probability with which a node enters into the failed state due to its inability to improve energy level
μ_{F}^{S}	Mean rate of nodes moving from failed node to selfish node
$\lambda_{O\_PM}^{C}$	Arrival rate of operating selfish nodes entering into cooperative state in spite of using Preventive Maintenance (PM) approach
λ_{F}^{S}	Mean rate of nodes moving from failed to selfish mode

3.2 Computation of Transition Function based on Associated Comprehensive States of a Node

The transition states of a node in the process of routing in a sensor networks are shown in Figure 1. In addition, the state types in the transition diagram are detailed below.

The state diagram of the propounded MPOTFEM is used for developing the steady state balance equations to predict the stochastic probabilities of node states (Figure 1). The Stochastic Steady State Probabilities (S^3P) connected with their compliant states with minimum likelihood to be transformed into other states are shown in Equations (1) and (2) correspondingly.

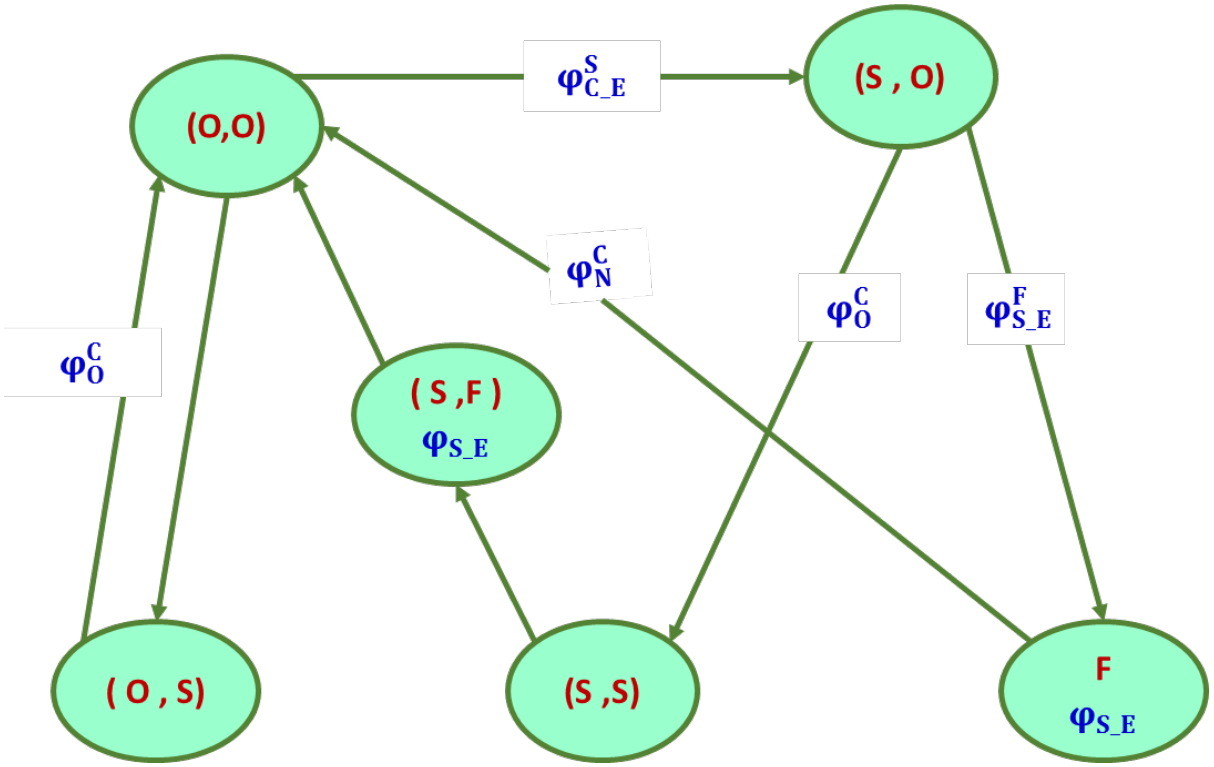

Figure 1. State Transition Diagram of the Propounded MPOTFEM Scheme

$$\left(\varphi^{S}_{C\_E} + \varphi^{F}_{S\_E}\right).\varphi^{S,F}_{C} = \varphi^{C}_{N}.\varphi^{F}_{S} + \beta.\varphi^{C,S}_{F\_E} + \varphi^{C}_{O}.\varphi^{C}_{S} \quad (1)$$

$$\varphi^{S,F}_{C} = \frac{\left(\varphi^{C}_{N}.\varphi^{F}_{S} + \beta.\varphi^{C,S}_{F\_E} + \varphi^{C}_{O}.\varphi^{C}_{S}\right)}{\left(\varphi^{S}_{C\_E} + \varphi^{F}_{S\_E}\right)} \quad (2)$$

The S^3P values of nodes related to the cooperative states with maximum possibilities to be transformed into selfish states are shown in Equations (3) and (4) correspondingly.

$$\varphi^{C}_{O}.\varphi^{C}_{S} = \varphi_{S\_E}.\varphi^{S,F}_{C} \quad (3)$$

$$\varphi^{C}_{S} = \frac{\varphi_{S\_E}.\varphi^{S,F}_{C}}{\varphi^{C}_{O}} \quad (4)$$

The S^3P values related to selfish nodes with maximum possibilities of being transformed into cooperative state are shown in Equations (5) and (6) correspondingly.

$$\left(\varphi^{F}_{S\_E} + \varphi^{C}_{O}\right).\varphi^{F,O}_{S} = \varphi^{S}_{C\_E}.\varphi^{S,F}_{C} \quad (5)$$

$$\varphi^{F,O}_{S} = \frac{\varphi^{S}_{C\_E}.\varphi^{S,F}_{C}}{\left(\varphi^{F}_{S\_E} + \varphi^{C}_{O}\right)} \quad (6)$$

The S^3P values related to the selfish nodes with maximum possibilities to fail are shown in Equations (7) and (8) correspondingly.

$$\varphi^{C}_{N}.\varphi^{F}_{S} = \varphi^{C}_{O}.\varphi_{S} \quad (7)$$

$$\varphi^{F}_{S} = \frac{\varphi^{C}_{O}.\varphi_{S}}{\varphi^{C}_{N}} \quad (8)$$

The S^3P values related to selfish nodes with maximum possibilities to maintain their states are shown in Equations (9) and (10) correspondingly.

$$\varphi^{C}_{O}.\varphi_{S} = \varphi_{S\_E}.\varphi^{F,O}_{S} \quad (9)$$

$$\varphi_{S} = \frac{\varphi_{S\_E}.\varphi^{F,O}_{S}}{\varphi^{C}_{O}} \quad (10)$$

The above-mentioned steady state equations are used for enumerating the stochastic values of 'φ_S', 'φ^{F}_{S}' and '$\varphi^{C,S}_{F\_E}$' states based on the cooperative state '$\varphi^{S,F}_{C}$' as shown in Equations (11-13) correspondingly.

$$\varphi_{S} = \frac{\varphi_{S\_E}}{\varphi^{C}_{O}} * \frac{\varphi^{S}_{C\_E}}{\left(\varphi^{F}_{S\_E} + \varphi_{S\_E}\right)} \varphi^{S,F}_{C} \quad (11)$$

$$\varphi^{F}_{S} = \frac{\varphi^{C}_{O}}{\varphi^{C}_{N}} * \frac{\varphi^{S}_{C\_E}}{\left(\varphi^{F}_{S\_E} + \varphi_{S\_E}\right)} \varphi^{S,F}_{C} \quad (12)$$

$$\varphi^{C,S}_{F\_E} = \frac{\varphi^{F}_{S\_E}}{\beta} * \frac{\varphi^{S}_{C\_E}}{\left(\varphi^{F}_{S\_E} + \varphi_{S\_E}\right)} \varphi^{S,F}_{C} \quad (13)$$

Furthermore, '$\varphi_C^{S,F}$' signifies the S^3P values of nodes in co-operative state. This probability completely exhibits the uptime to which the nodes could continue to be compliant with the network as shown in Equation (14).

$$\varphi_C^{S,F} = \frac{1}{\left(1+\left(\left(1+\frac{\varphi_{S\_E}^F}{\beta}+\frac{\varphi_{S\_E}}{\beta}+\frac{\varphi_{S\_E}}{\mu}\right)\frac{\varphi_{C\_E}^S}{(\varphi_{C\_E}^S+\varphi_{S\_E})}\right)+\frac{\varphi_{S\_E}}{\varphi_O^C}\right)} \quad (14)$$

However, the nodes are considered to be accessible in the network based on their up and down times during which, service is enabled for data propagation. Thus, in the process of estimating the Opportunistic factor in the proposed mechanism, the up and down times of nodes are calculated and combined.

3.3 Estimation of Markov Process-based Opportunistic Trust Factor (MPOTF)

The probability of node state to be possibly transited to the operating state is shown in Equation (15). The propounded scheme is based on the Preventive Maintenance (PM) approach for retrieval of the potential after downtime.

$$\varphi_{PM}^O = \frac{\varphi_{S\_E}}{\varphi_O^C}\,\varphi_S^C \quad (15)$$

In this perspective, the probability of the node entering into a failed state despite employing PM approach is shown in Equation (16).

$$\varphi_{F\_PM}^S = \frac{\varphi_{S\_E}^F}{\varphi_O^C}\,\varphi_S^C \quad (16)$$

At this point, the cumulative sum of probability relating to the probable states of the node at any definite point of time is computed using the rule of probability as shown in Equation (17).

$$\varphi_C^{S,F} + \varphi_{PM}^O + \varphi_{F\_PM}^S = 1 \quad (17)$$

Hence, the probabilities with which the nodes exhibit a complete operating behavior is recognized based on simultaneous equations as shown in Equation (18).

$$\varphi_{O\_PM} = \frac{\varphi_{O\_PM}^C * \varphi_{F\_PM}^S}{(\varphi_{O\_PM}^C * \varphi_{F\_PM}^S)+(\varphi_{S\_E} * \varphi_{F\_PM}^S)+(\varphi_{F\_E}^S * \varphi_{O\_PM}^C)} \quad (18)$$

The Markov Process-based Opportunistic Trust Factor (φ_{MPOTF}) is computed by taking into account the failure and non-failure states of nodes as shown in Equation (19).

$$\varphi_{MPOTF} = \frac{\mu_{O\_PM}^C * \mu_F^S}{(\mu_{O\_PM}^C * \mu_F^S)+(\lambda_{O\_PM}^C * \mu_F^S)+(\lambda_F^S * \mu_{O\_PM}^C)} \quad (19)$$

The mean rate of transforming a non-operating node into an operating node is shown in Equation (20).

$$\mu_{NO}^O = \frac{1}{\varphi_{S\_E}} \quad (20)$$

Furthermore, the mean rate of a node being reformed from its failed to operating state is given in Equation (21).

$$\mu_{MPOTF\_PM} = \frac{\varphi_{F\_PM}^S}{\left(\left(\frac{\varphi_{F\_PM}^S}{\varphi_{MPOTF}}\right)-(\mu_{O\_PM}^C * \varphi_{F\_PM}^S)-(\varphi_{F\_E}^S * \mu_{O\_PM}^C)\right)} \quad (21)$$

where, 'φ_{PAFTF_PM}' is in the range '0' and '1'. Moreover, the time required for rehabilitating a node from its failed state is found using Equation (19) by considering the failure and repair rates, Opportunistic threshold and PM cost of nodes. The value of 'φ_{PAFTF_PM}' should be more than 0.80 for a node to be elected as the CH.

3.4 Algorithm and complexity of the Proposed MPOTFEM

This section details about the algorithm and flowchart of the proposed MPOTFEM.

Input: RE, location of nodes, trust enumerated using packet forwarding competence
Output: Optimized CHs for improving the network's lifespan and energy stability

Begin
Initialize the number, energy and location of nodes
Consider the positioned nodes' states as primarily compliant with the number of CHs set to 'Φ'
Compute the number of adjoining nodes depending on the total number of nodes that are alive till the former iteration
Estimate the trust and energy limit based on the utilized energy and trust model
Compute the transition probabilities for enumerating the trust factor of the nodes based on 'φ_{S_E}', '$\varphi_{C\_E}^S$', '$\varphi_{S\_E}^F$', 'β', 'φ_O^C' and 'φ_N^C' for exploring the features of nodes
Find the stochastic probability vectors '$\varphi_C^{S,F}$', 'φ_S^C', '$\varphi_S^{F,O}$', 'φ_S^F', 'φ_S' and '$\varphi_{F\_E}^{C,S}$' for enumerating 'φ_{PAFTF_PM}' so as to accomplish enhanced CH selection
If the value of 'φ_{PAFTF_PM}' associated with the explored node is more than the estimated CH selection threshold of 0.80
Select the appropriate nodes as CHs and initiate clustering
Transmit the information about the new CH to other collaborating nodes
Else
Upsurge the number of rounds by 1 and explore the nodes based on the Opportunistic factor
End If

End

The aforementioned algorithm considers a pre-determined CH selection threshold of 0.80, which is taken as the Opportunistic factor. This threshold is determined by conducting experiments for varying number of thresholds ranging from 0.60 to 0.90. Energy efficient and trusted CH selection is fairly better only after 0.80. In addition, the threshold supports suitable individuality between operating and non-operating states of nodes. Compared to the HGRF-OCHP technique, the computation complexity of the propounded scheme is also found to be of the order O(n log n) with control message complexity of O(n) and time complexity of O(1) correspondingly.

3.5 Flowchart illustrating the steps in the Proposed MPOTFEM

The flowchart shows the steps of the propounded MPOTFEM (Figure 2).

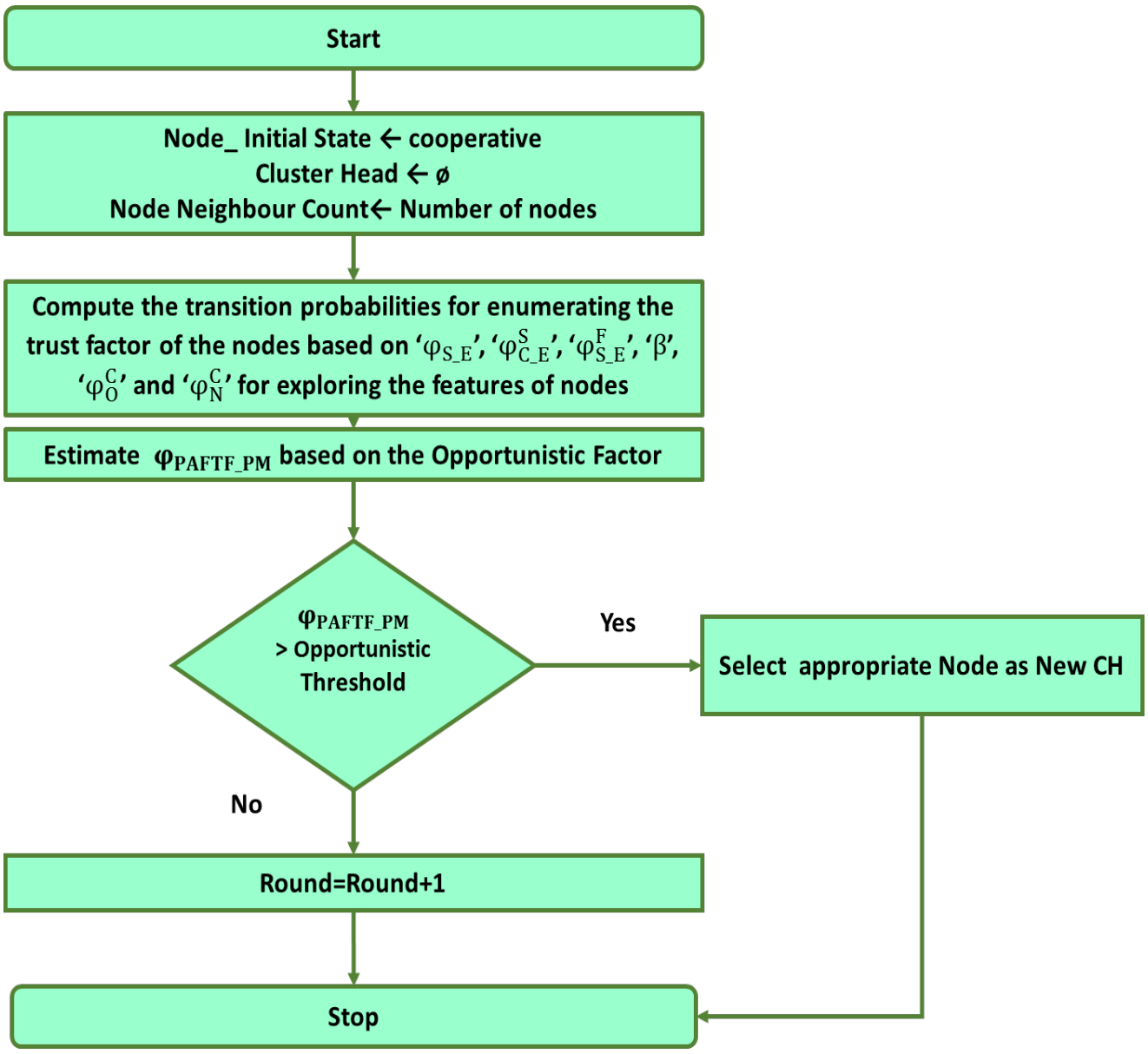

Figure 2. Flowchart of the Proposed MPOTFEM Scheme

4 Simulation Results and Discussions

The propounded Markov Process-based Opportunistic Trust Factor Estimation Mechanism (MPOTFEM) and the benchmarked HGRF-OCHP, TAREEN-OCHS, EEST-OCHS and TL-LEACH schemes are simulated using ns-2.35. A terrain of 100*100 meters with 1000 nodes is taken. Random Way Point (RWP) and bidirectional models are employed for mobility and communication respectively. The parameters taken for implementation of the existing [20-22] and propounded schemes are shown in Table 2.

Simulation is carried out based on different factors. Initially, the performance of the proposed MPOTFEM is assessed in terms of percentages of alive and dead nodes, average RE and average throughput for varying number of rounds of implementation. Secondly, the performance of the proposed and the benchmarked schemes is estimated in terms of Packet Delivery Ratio (PDR), Failure Rate, mean rate of malicious modes to be selected as CH and average Delay for varying percentages of malicious nodes. Thirdly, the performance is examined in terms of average throughput, average delay, average prevention rate and average RE of malevolent nodes to be nominated as the CH for varying number of nodes. Finally, the performance of the proposed approach is assessed based on network lifetime and communication overhead for varying number of nodes positioned in the network.

Table 2. Simulation Parameters

Parameters	Values
Simulation Area	400*400 meters
Number	1000
Initial Energy	0.5 Joules
Speed	1-10 m/s
Length of control packets (bytes)	50
Length of data packets (bytes)	512
Queue category	Drop tail
Size of packets (bits)	2000
Sensing Interval (msec)	0.01
Time taken for simulation (sec)	600

4.1 Investigation based on Varying Number of Rounds of Implementation

In the initial part of examination, the proposed MPOTFEM scheme is evaluated based on the percentage of alive and dead nodes, average RE and average throughput for varying number of rounds of implementation. Figure 3 and Figure 4 show the percentage of alive and dead nodes in the network or varying number of rounds of implementation respectively.

The percentage of alive nodes in a network with the proposed MPOTFEM scheme is seen to be better in contrast to the existing CH election mechanisms take for examination. This substantial improvement in the performance of the proposed mechanism is predominantly due to the estimation of the Opportunistic factor that supports estimation of the importance of nodes. The proposed MPOTFEM offers 7.54%, 8.92%, 10.86% and 12.56% better percentage of alive nodes in contrast to HRFCHE, EEST-CHST and HDEEHC schemes (Figure 3).

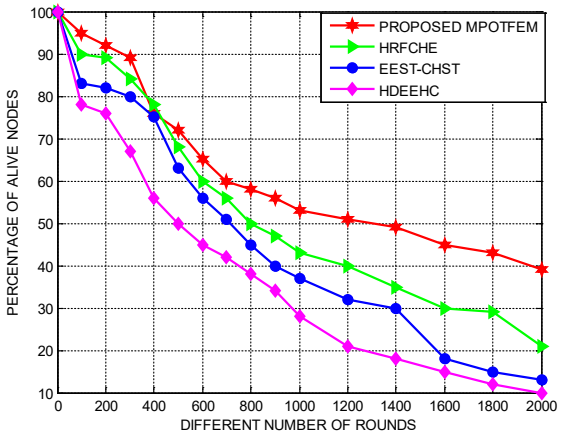

Figure 3. Percentage of Alive Nodes for Varying Rounds of Implementation

Likewise, the percentage of dead nodes is found to be reduced in the proposed MPOTFEM as it involves less energy in the network by involving Preventive Maintenance (PM) strategy. The percentage of dead nodes of the proposed MPOTFEM are also 7.32%, 8.94%, 9.68% and 10.27% better when compared to the existing HRFCHE, EEST-CHST and HDEEHC schemes (Figure 4).

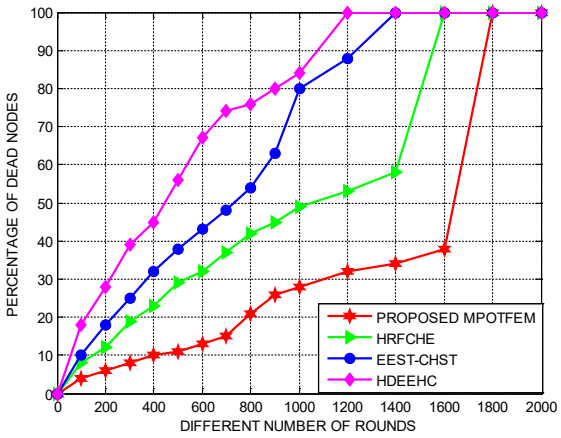

Figure 4. Percentage of Dead Nodes for Varying Rounds of Implementation

Figure 5 and 6 show the average throughout and average RE for varying number of rounds of implementation. The average throughput of the proposed MPOTFEM scheme is found to be better when compared baseline CH election mechanisms. The substantial improvement in average throughput of the propounded MPOTFEM is possible due to the inhibition of selection of malevolent nodes from being elected as CH nodes. The average throughput offered by the proposed MPOTFEM is seen to be 8.28%, 9.75%, 11.28% and 12.96% better when compared to the existing HRFCHE, EEST-CHST and HDEEHC approaches (Figure 5).

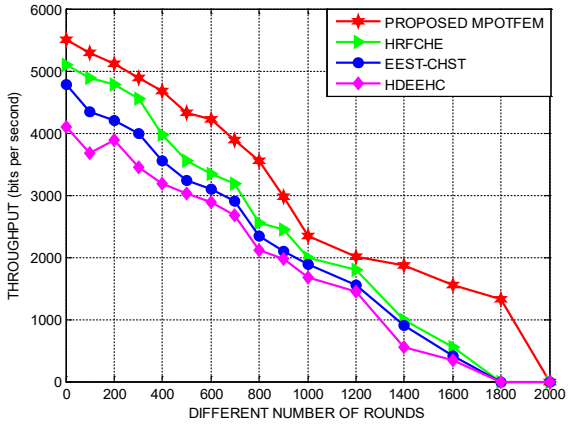

Figure 5. Average Throughput for Varying Rounds of Implementation

Likewise, the proposed MPOTFEM approach maintains average RE of the network to a greater extent as PM process of reorienting nodes. The average RE sustained by the proposed MPOTFEM is 9.12%, 10.64%, 11.84% and 14.29% better when compared to the existing HRFCHE, EEST-CHST and HDEEHC (Figure 6).

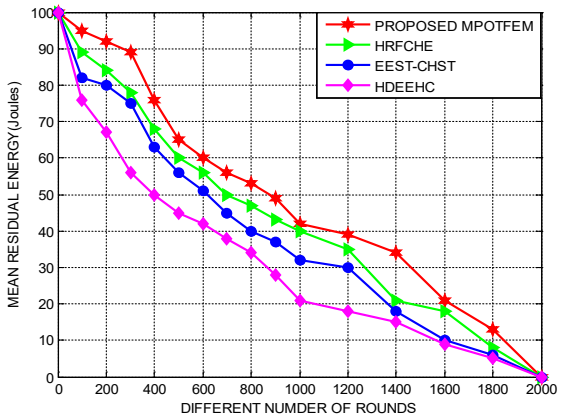

Figure 6. Average Residual Energy for Varying Rounds of Implementation

4.2 Investigation based on Varying Percentage of Malicious Nodes

In the second part of examination, the proposed MPOTFEM scheme is evaluated based on PDR, failure rate, average rate of malicious nodes elected as CH and average delay for varying percentage of malicious nodes. Figure 7 shows the PDR of the proposed and the compared schemes. The PDR of the propounded MPOTFEM scheme is better in contrast to the existing CH selection mechanisms independent of the number of malevolent nodes. Improvement in PDR is primarily due to the Markov process that is capable of predicting the nodes with high Opportunistic factor. The PDR of the proposed MPOTFEM scheme is found to be CH selection techniques.

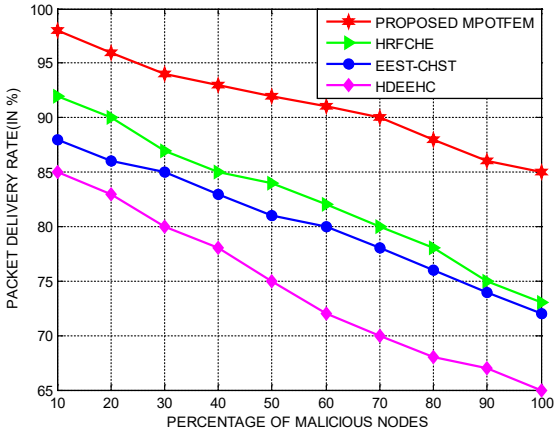

Figure 7. Packet Delivery Ratio for Varying Percentage of Malicious Nodes

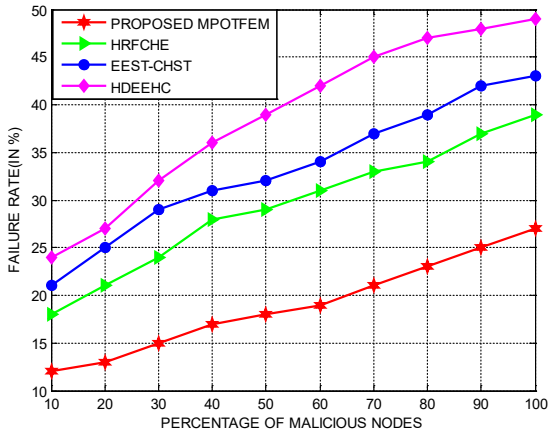

Figure 8. Failure Rate for Varying Percentage of Malicious Nodes

In addition, Figure 8 shows the failure rate of the proposed and the existing schemes. The failure rate of the nodes of the proposed mechanism is found to be minimal when compared to the existing CH selection approaches not based on the number of malevolent nodes introduced in the network. This probable decrease in the failure rate of the proposed mechanism is predominantly due to the improved degree of prevention rate introduced by the MATF parameter that classifies nodes into cooperative, selfish and failed. The proposed offers 8.54%, 9.65%, 10.54% and 11.84% reduced failure rate in contrast to the existing HRFCHE, EEST-CHST and HDEEHC CH selection techniques.

Figure 9 shows the average rate of malevolent nodes elected as CH in the propounded and existing CH election mechanisms. The probability of a malicious nodes getting elected as the CH is reduced in the proposed MPOTFEM scheme when compared to the existing CH election mechanisms independent of the number of malevolent nodes hosted in the network. Preventing malicious nodes from being elected as CHs is possible due to the non-operating and operating states of Markov process taken for prediction. The prevention rate of malevolent nodes of the proposed MPOTFEM scheme is 8.21, 9.54%, 10.42% and 12.29% reduced in contrast to the existing CH election mechanisms.

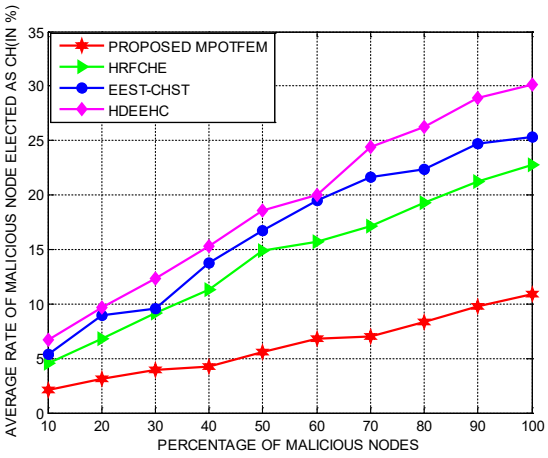

Figure 9. Average Rate of Malicious Nodes Elected as CH for Varying Percentage of Malicious Nodes

Furthermore, Figure 10 shows the average delay experienced by the proposed and the existing schemes. The proposed mechanism involves less average delay due to the high exploration competency forced on the nodes in CH selection. The average delay of the proposed mechanism is seen to be 7.94%, 8.72%, 9.64% and 10.98% less in contrast to the existing CH election mechanisms.

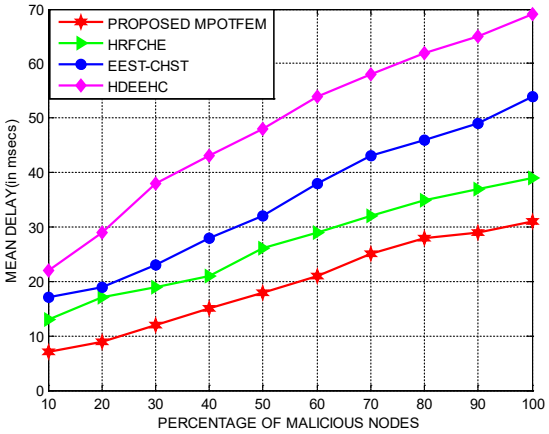

Figure 10. Average Delay for Varying Percentage of Malicious Nodes

4.3 Investigation based on Varying Number of Nodes

In the third fold of investigation, the predominance of the propounded scheme is based on percentage enhancement in average throughput, percentage sustenance of average RE, average delay and average inhibition rate of malevolent nodes to be elected as the CH for increasing number of nodes.

Figure 11 shows the percentage upsurge in average throughput of the proposed and the existing schemes for varying number of nodes. There is a percentage increase in the throughput of the proposed mechanism when compared to the existing CH election mechanisms as it includes the benefits of including the Opportunistic factor using the continuous Markov chain process for effective election of CH. The proposed mechanism offers 8.28%, 9.74%, 10.52% and 12.74% better average throughput in contrast to the existing HRFCHE, EEST-CHST and HDEEHC schemes.

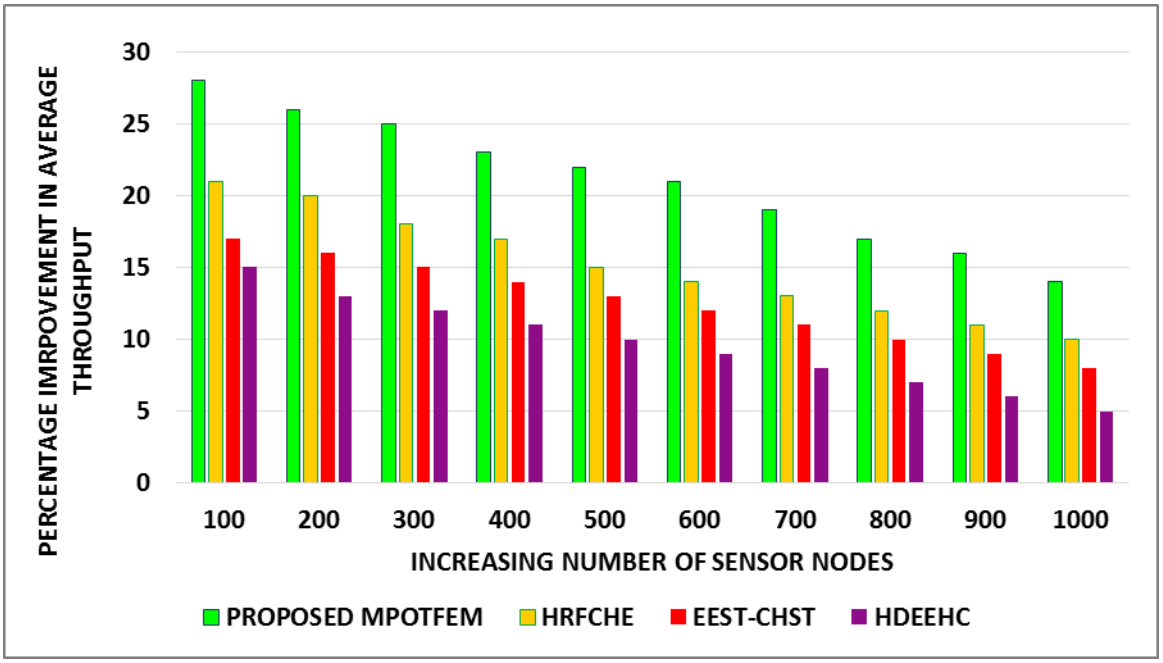

Figure 11. Percentage Improvement in Average Throughput for Varying Number of Nodes

In addition, Figure 12 shows the percentage sustenance in the average RE of the proposed and the existing CH election mechanisms for varying number of nodes. This improved percentage sustenance in the proposed MPOTFEM scheme is found to be better when compared to the existing CH selection approaches, as it utilizes the Opportunistic parameter in CH selection. The average RE sustenance of the proposed MPOTFEM scheme is found to be 8.82%, 11.84%, 12.92% and 13.82% better in contrast to the HRFCHE, EEST-CHST and HDEEHC selection schemes.

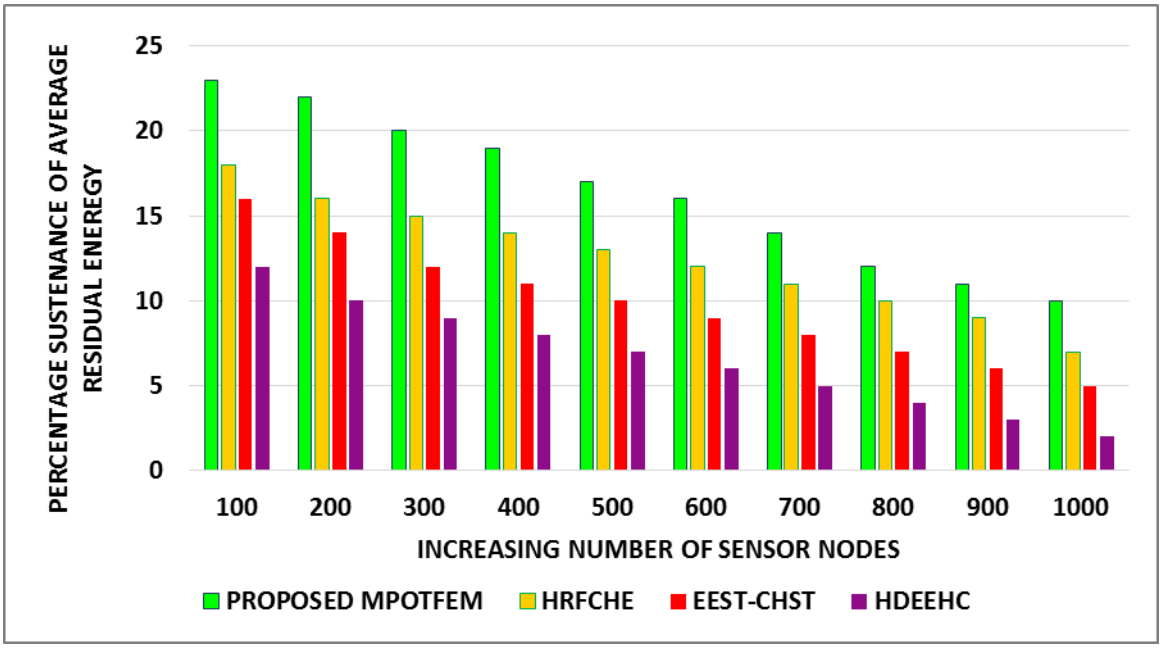

Figure 12. Percentage Sustenance of Average Residual Energy for Varying Number of Nodes

Furthermore, Figure 13 shows the average delay of the proposed MPOTFEM and prevalent CH election mechanisms for increasing number of nodes. The average delay of the proposed mechanism is found to be

reasonably low in contrast to other CH election mechanisms as it circumvents least energy competent nodes from being elected as the CH. The average delay of the proposed MPOTFEM scheme is found to be 8.73%, 10.28%, 11.32% and 12.84% better in contrast to HRFCHE, EEST-CHST and HDEEHC selection schemes.

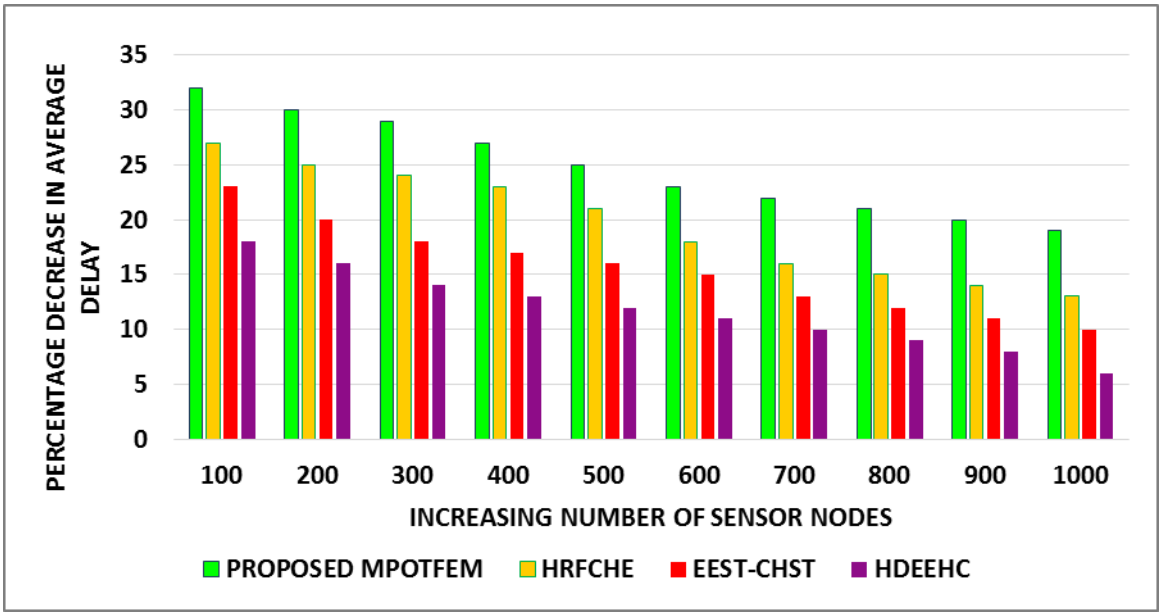

Figure 13. Average Delay for Varying Number of Nodes

In addition, the mean prevention rate of malevolent nodes from being elected as the CH in the proposed MPOTFEM and the CH election mechanisms for varying number of nodes is shown in Figure 14. The mean prevention rate of malevolent nodes from being elected as the CH is guaranteed to be less in the proposed scheme when compared to the other CH election approach as it is capable of classifying the states of nodes based on trust and energy. The proposed MPOTFEM scheme offers 8.28%, 9.48%, 11.13% and 12.64% better mean prevention rate in contrast to the existing HRFCHE, EEST-CHST and HDEEHC selection schemes.

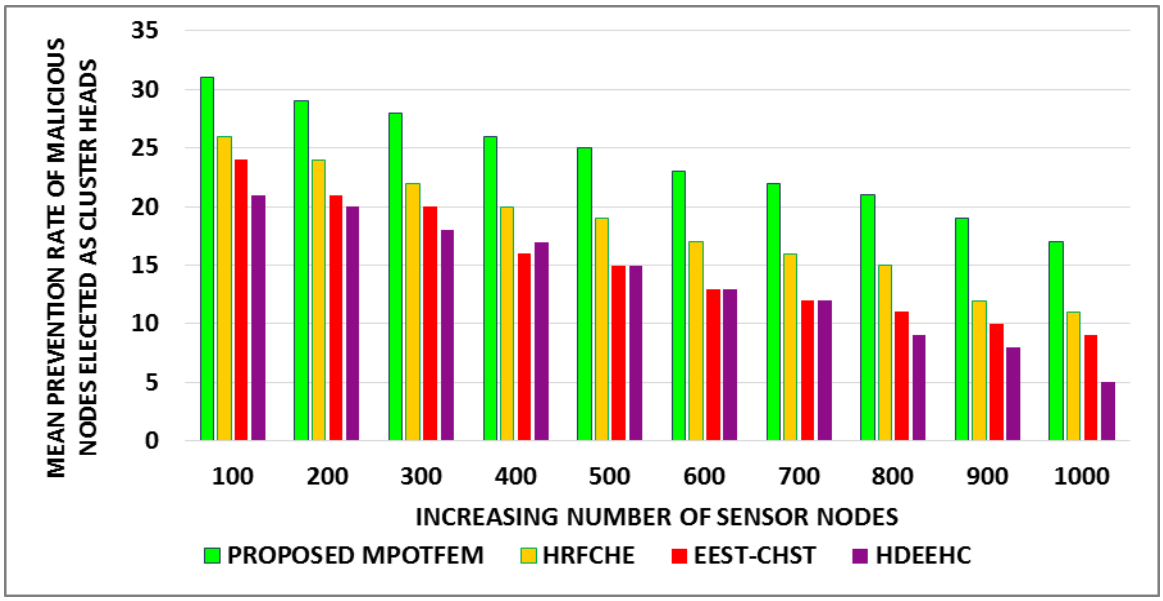

Figure 14. Mean Prevention Rate of Malicious Nodes Elected as CH for Varying Number of Nodes

The proposed MPOTFEM scheme is examined in terms of percentage increase and decrease in network lifetime and communication overhead respectively for varying number of nodes. The proposed MPOTFEM scheme offers 7.21%, 9.28%, 11.46% and 12.94% percentage increase in network lifetime for varying number of nodes in contrast to the HRFCHE, EEST-CHST and HDEEHC selection schemes (Figure 15).

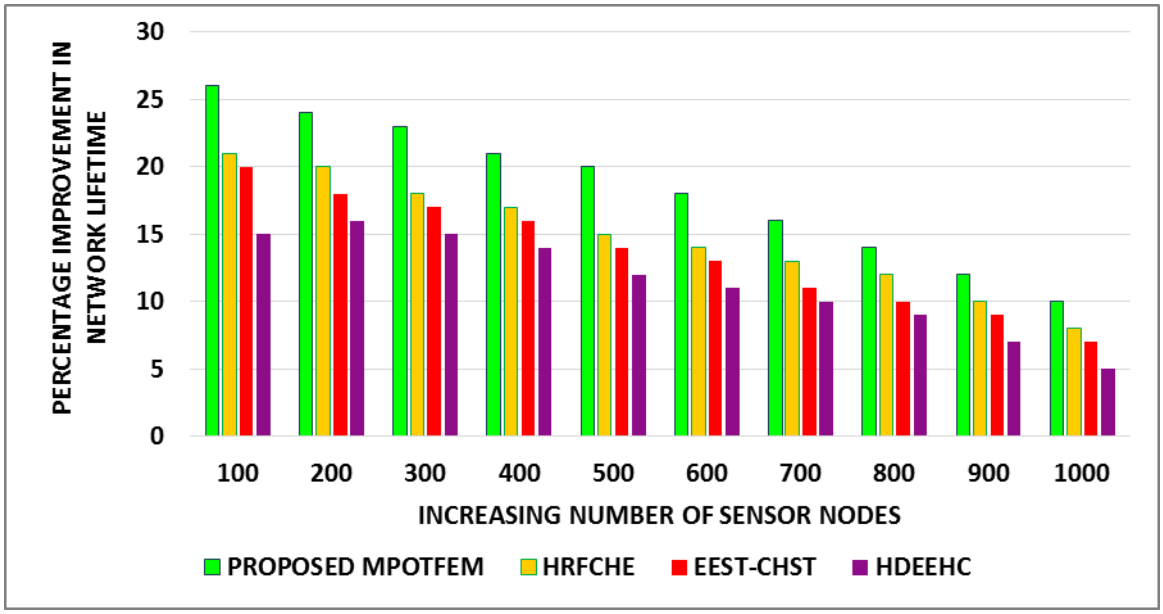

Figure 15. Percentage Increase in Network Lifetime for Varying Number of Nodes

Similarly, the proposed MPOTFEM scheme offers 6.91%, 7.98%, 8.54% and 10.28% percentage decrease in communication overhead for varying number of nodes in contrast to HRFCHE, EEST-CHST and HDEEHC clustering approaches. The percentage increase and decrease in network lifetime and communication overhead of the proposed MPOTFEM scheme is primarily due to the use of the Opportunistic parameter (Figure 16).

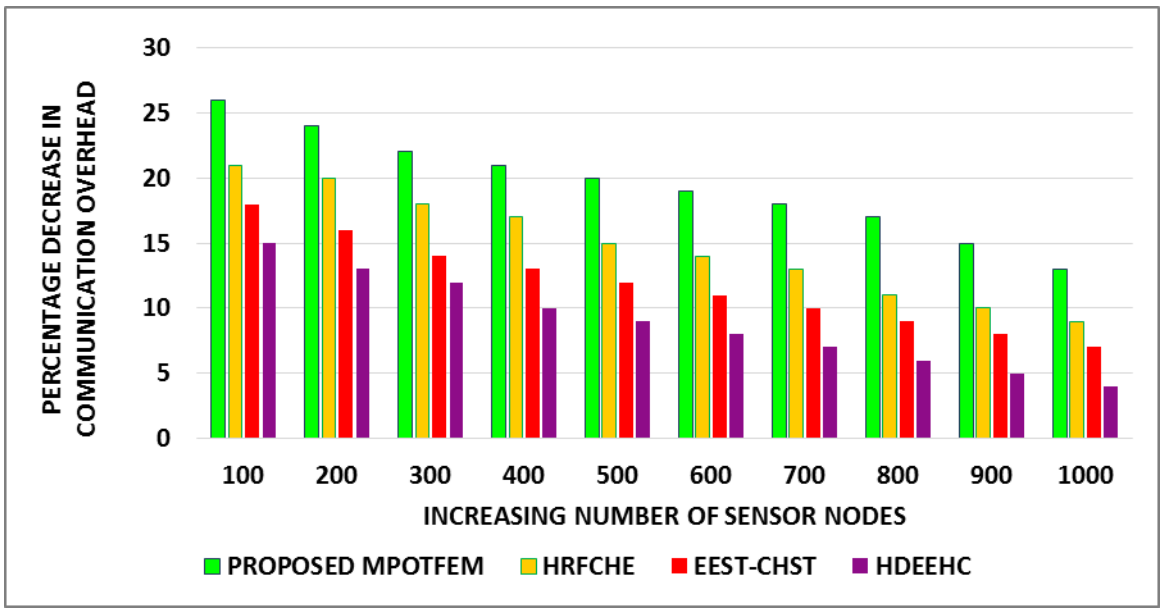

Figure 16. Percentage Decrease in Communication Overhead for Varying Number of Nodes

5. Conclusion

The proposed Markov Process-based Opportunistic Trust Factor Estimation Mechanism (MPOTFEM) is a trustworthy approach for electing appropriate Cluster Head (CH) based on the use of Opportunistic parameter. This proposed MPOTFEM scheme includes Markov chain and Preventive Maintenance (PM) concept for assessing the degree to which the network is serviced. It is seen that, malevolent nodes are not elected as CHs by mitigating frequent election of CHs. From the simulation results, it is seen that the proposed mechanism is prime in sustaining the percentage of alive and dead nodes in the network by 10.82% and 11.36% on average in contrast to the existing schemes. The results show that the proposed mechanism is competent in offering 9.14% and 10.56% improved PDR and Throughput on average in contrast to the prevalent CH election mechanisms.

References

[1] Rajarajeswari, P. L., Karthikeyan, N. K., & Priya, M. D. (2015). EC-STCRA: Energy Conserved–Supervised Termite Colony based Role Assignment scheme for Wireless Sensor Networks. Procedia Computer Science, 57, 830-841.

[2] Janakiraman, S. (2018). A hybrid ant colony and artificial bee colony optimization algorithm-based cluster head selection for iot. Procedia computer science, 143, 360-366.

[3] Rambabu, B., Reddy, A. V., & Janakiraman, S., (2019) A Hybrid Artificial Bee Colony and Bacterial Foraging Algorithm for Optimized Clustering in Wireless Sensor Network., Vol.8, No. 10, pp. 2186-2190.

[4] Rambabu, B., Reddy, A. V., & Janakiraman, S. (2019). Hybrid Artificial Bee Colony and Monarchy Butterfly Optimization Algorithm (HABC-MBOA)-based cluster head selection for WSNs. Journal of King Saud University-Computer and Information Sciences.

[5] Priya, M. D., Suganya, T., Malar, A. C. J., Dhivyaprabha, E., Prasad, P. K., & Vardhan, L. V. (2020). An Efficient Scheduling Algorithm for Sensor-Based IoT Networks. In Inventive Communication and Computational Technologies (pp. 1323-1331). Springer, Singapore.

[6] Janakiraman, S., Priya, M. D., (2020). An Energy-Proficient Clustering-Inspired Routing Protocol using Improved Bkd-tree for Enhanced Node Stability and Network Lifetime in Wireless Sensor Networks. International Journal of Communication Systems, 33(16), e4575.

[7] Taheri, H., Neamatollahi, P., Younis, O. M., Naghibzadeh, S., & Yaghmaee, M. H. (2012). An energy-aware distributed clustering protocol in wireless sensor networks using fuzzy logic. Ad Hoc Networks, 10(7), 1469-1481.

[8] Wang, S. S., & Chen, Z. P. (2012). LCM: A link-aware clustering mechanism for energy-efficient routing in wireless sensor networks. IEEE sensors journal, 13(2), 728-736.

[9] Wang, J., Zhu, X., Cheng, Y., & Zhu, Y. (2013). A distributed, hybrid energy-efficient clustering protocol for heterogeneous wireless sensor network. International Journal of Grid and Distributed Computing, 6(4), 39-50.

[10] Xu, Z., Chen, L., Cao, L., Liu, T., Yang, D., & Chen, C. (2015). DARC: A distributed and adaptive routing protocol in cluster-based wireless sensor networks. International Journal of Distributed Sensor Networks, 11(12), 627043.

[11] Thilagavathi, S., & Gnanasambandan Geetha, B. (2015). Energy aware swarm optimization with intercluster search for wireless sensor network. The Scientific World Journal, 2015.

[12] Zhou, H., Wu, Y., Feng, L., & Liu, D. (2016). A security mechanism for cluster-based WSN against selective forwarding. Sensors, 16(9), 1537.

[13] Wang, T., Zhang, G., Yang, X., & Vajdi, A. (2016). A trusted and energy efficient approach for cluster-based wireless sensor networks. International Journal of Distributed Sensor Networks, 12(4), 3815834.

[14] Miglani, A., Bhatia, T., Sharma, G., & Shrivastava, G. (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.

[15] Amuthan, A., & Arulmurugan, A. (2018). An availability predictive trust factor-based semi-Markov mechanism for effective cluster head selection in wireless sensor networks. International Journal of Communication Systems, pp. 1-16.

[16] Amuthan, A., & Arulmurugan, A. (2018). Semi-Markov inspired hybrid trust prediction scheme for prolonging lifetime through reliable cluster head selection in WSNs. Journal of King Saud University-Computer and Information Sciences. pp.34-46.

[17] Mythili, V., Suresh, A., Devasagayam, M. M., & Dhanasekaran, R. (2019). SEAT-DSR: Spatial and energy aware trusted dynamic distance source routing algorithm for secure data communications in wireless sensor networks. Cognitive Systems Research, 58, 143-155.

[18] Rodrigues, P., & John, J. (2020). Joint trust: an approach for trust-aware routing in WSN. Wireless Networks, 1-16.

[19] Sharma, R., Vashisht, V., & Singh, U. (2020). eeTMFO/GA: a secure and energy efficient cluster head selection in wireless sensor networks. Telecommunication Systems, 1-16.

[20] Poluru, R. K., & Ramasamy, L. K. (2020). Optimal cluster head selection using modified rider assisted clustering for IoT. IET Communications, 14(13), 2189-2201.

[21] Panda, S., Behera, T. M., Samal, U. C., & Mohapatra, S. K. (2020). Modified threshold for cluster head selection in WSN using first and second order statistics. IET Wireless Sensor Systems, 10(6), 292-298.

[22] Shivappa, N., & Manvi, S. S. (2019). Fuzzy-based cluster head selection and cluster formation in wireless sensor networks. IET Networks, 8(6), 390-397.