A Stable Clustering Scheme with Node Prediction in MANET

S. R. Drishya[1], Renuka Devi. S[2] and Vaidehi. V[3]

[1]School of Computing Science and Engineering, VIT University, Chennai, India
[2]School of Computing Science and Engineering, VIT University, Chennai, India
[3]Department of Computer Science, Mother Theresa Women's University, Kodaikanal, India

***Abstract*:** The main concern in MANET is increasing network lifetime and security. Clustering is one of the approaches that help in maintaining network stability. Electing an efficient and reliable Cluster Head (CH) is a challenging task. Many approaches are proposed for efficient clustering, weight-based clustering is one among them. This paper proposes a stable clustering scheme which provides network stability and energy efficiency. Proposed Stable Clustering Algorithm with Node Prediction (SCA-NP) computes the weight of the node using a combination of node metrics. Among these metrics, Direct Trust (DT) of the node provides a secure choice of CH and Node Prediction metric based on the minimum estimated time that node stay in the cluster provides the stable clustering. Mobility prediction is considered as the probability that a node stays in the network. This metric helps in electing CH which is available in the network for a longer time. Simulation is done in NS3 to evaluate the performance of SCA-NP in terms of clusters formed, network lifetime, efficiency in packet delivery, detecting malicious nodes and avoiding them in communication

***Keywords*:** Weight based clustering, Stable clustering, Direct Trust, Mobile prediction, Minister Node,

1. Introduction

MANET comprises of nodes having constraints on energy, bandwidth, resources and more. When the number of nodes in the network is large, the managing of the network becomes hard due to its dynamic nature and self-organizing capability [32, 33]. Providing communication for MANET efficiently and securely is one of the major challenging tasks [1]. To provide good communication, nodes in a geological location formed into groups called clusters. Dividing the complete network into clusters helps in efficiently managing MANET. The technique of forming clusters is termed as clustering. Clustering also helps to provide better communication among constrained nodes in the network. Each cluster consists of Cluster Head (CH), cluster members and gateway nodes [34]. Many clustering techniques were evolved and many researches are going on this context but MANET sustainable clustering technique is yet to evolve.

Clustering can be done on many characteristics of nodes such as Node ID, Spatial and temporal locations, mobility of the node, weight of the nodes, the trustworthiness of the nodes etc. Among all the techniques, clustering based on the weight will be optimal due to the consideration of many features of the node at once. Weight of the node includes the velocity of the node, residual energy, degree of the node, transmission ranges etc. [35]. As almost all features of the nodes are considered in weight calculation, the elected CH will be efficient among all the nodes in the cluster.

Clustering techniques are classified into two types based on security as Insecure clustering and Secure Clustering. Insecure clustering techniques assume that the network is fully trusted or ignore the security of the network and forms the clusters. Clustering techniques like weight-based, mobility-based, location-based and channel-based clustering are insecure clustering techniques. All of these techniques ignore the concept of malicious nodes in the network. As far as MANET, security is the primary concern. In a secure clustering, the security of the network is considered. Trust-based clustering considers the evaluation of trustworthiness of the nodes to avoid malicious nodes. Cryptographic based clustering uses cryptographic algorithm to avoid outsider attack but fails to prevent insider attacks. The hybrid scheme provides high security to the network but facing problems like more energy consumption and communication overhead. Due to dynamic nature of MANET, providing efficient communication is still an issue.

After forming efficient clusters and electing CH, MANET is still facing problems such as re-clustering, communication overhead and link unavailability problems. So the prediction of node mobility comes to existence [17]. Many prediction algorithms were proposed and used to predict node behavior and act accordingly. Mobility prediction is a process of predicting node path or future location based on pre-observed behaviors. Main purpose of mobility prediction in MANET is to avoid routing overhead [2]. As of now, routing is done based on the shortest path. Due to nodes mobility, a link may be unavailable resulting in data loss and also rediscovering of new routes. So a stable path is needed for efficient communication. This can be achieved by predicting the availability of the nodes within the specific locations for a specific period [19].

The proposed clustering scheme, Stable Clustering Algorithm with Node Prediction (SCA-NP) considers many key features that are significant for efficient and reliable communication and clustering. Nodes in the network forms into clusters and CH are elected by considering both trust and weight of the nodes in clustering with mobility as a primary concern in weight calculation. For cluster maintenance, a minister node is selected to avoid re-clustering and also it involves mobility prediction technique to form stable routing for a particular moment.

The paper is organized as follows: Section 2 discusses related research done on weight-based clustering, Trust evaluation, and mobility prediction. Section 3 gives a detailed description of the proposed algorithm. Results and discussions are provided in section 4 and section 5 concludes the discussion.

2. Literature Survey

Trust is one of the primary concerns in Node evaluation in MANET. If trust is not considered, then the cluster cannot be stable for a longer time [3]. If trust is calculated, node behavior is known prior and it can be used for communication in a better way. In “ART:Attack-Resistant Trust Management Scheme for Securing Ad Hoc Networks” [21], a trust management scheme is proposed. The trustworthiness of a node is evaluated by both metrics: functional trust and recommendation trust. Functional trust is a metric to measure how efficiently a node can perform its functionalities and recommendation trust is how trustworthy the node recommendation about other nodes. Each node in the network knows functional and recommendation trust value of all other nodes. Nodes with high voting are suggested as trustable nodes.

In “A Trust Based Clustering Framework for Securing Ad Hoc Networks” **[10],** a clustering scheme is proposed based on trust. Trust is evaluated based on the behavior of the node. Certification mechanism is used to evaluate a node as trustable or not. If the node is marked as "suspicious" it has to get a certificate as trustable otherwise it is restricted in intracluster communication.

A Distributed and Adaptive Trust Evaluation Algorithm (DATEA) [5] subdivides the trust evaluation to communication trust and energy trust. Communication trust is calculated based on the number of packets communicated between nodes. Energy Trust is calculated based on the residual energy of nodes. Direct trust is calculated by communication and energy trust whereas indirect rust is calculated based on reliability and familiarity. Combining direct and indirect trust, final trust is calculated for a node.

In Energy Efficient Secure Trust based Clustering Algorithm [4], CH selection algorithm is proposed in which weight calculation is done with security and minimum energy consumption. Weight of the node includes trust as one of the metrics along with waiting time, degree of the node and distance among the nodes.

This paper considers weight-based clustering among all clustering schemes in MANET because these schemes involve the consideration of different key features of the node to elect an efficient CH. In “An Efficient Clustering Algorithm for MANET Based on Weighted Parameters” [11], the author H.Zhou, proposes an efficient clustering technique based on weighted parameters. This technique considers relative speed rather than obsolete speed in weight calculation to maintain the cluster stability and cluster structure. It also gives a chance to a node whether to join a cluster or not by comparing weights locally with each other.

Clustering based on weight is first proposed in “WCA : A Weighted Clustering Algorithm for Mobile” [8]. The algorithm calculates the weight of the nodes to adapt dynamically for ad hoc networks. Weight is calculated by considering different features of the node such as transmission power, ideal degree, battery power and mobility of the nodes. It also has the flexibility to assign different values to the weighing parameters in weight calculation. Node with the smallest weight becomes the CH.

A robust weighted clustering algorithm called PMW (Power-Mobility-Workload) [7] is proposed. This paper introduces the concept of relative mobility in weight calculation. If the node's mobility is considered, the direction of mobility cannot be assured. So, using relative mobility it is easy to predict the direction of nodes in the same direction or the opposite. Prediction of mobility direction helps in avoiding re-clustering.

ENB (Energy- Node connectivity- Bandwidth) is a Cluster Head election algorithm proposed in [18]. It considers residual energy, connectivity of the node and available bandwidth for weight calculation. Node with highest weigh becomes CH.

An Energy Efficient and Safe Weighted Clustering Algorithm is proposed by D. Amine, B. Nassreddine, and K. Bouabdellah [16] which introduces Behavioral Level (BL) of a node in weight calculation. BL of a node is defined equally to all the nodes as 1. If the node shows any misbehavior then BL is decreased based on the performance. If a node is having BL less than a threshold value it cannot be accepted as CH.

K. Wang and B. Li [22] proposes a velocity-based mobility group model and based on the parameters of the mobility model, the future network partitioning is predicted. The ad hoc network with dispersed and mixed nodes is considered. The occurrence of the partition is predicted as a sequence of the expected time of separation between the various pairs of mobility groups in the network. For eg., an ad-hoc network with mobility groups C_1, C_2 and C_3, the network is predicted to partition at times $t = T_{12}$, T_{13} and T_{23}. Since RVGM predicts the partitioning of the network where each partition group forms a cluster we say the prediction is applied at the Cluster formation stage.

In “Energy efficient cluster based mobility prediction for wireless sensor networks” [23], the position estimation of each mobile sensor is done by the node itself. The mobile sensor nodes calculate their position using Kalman filter and send the State Update which consists of acceleration, velocity and their position to the CH. The CH will, in turn, send this information to the sink node. Before receiving the information from the CH, the sink would predict the location of the mobile sensors using geographical routing and compare the results obtained from the CH. Finally, the sink node sends the data to the mobile sensor nodes after determining the position of the sensor nodes. The sink sends data to the mobile nodes based on the predicted location of the nodes. If the location of the node is changed then the node would belong to the next cluster. Hence, we classify this approach as prediction applied during cluster maintenance.

“Qos in manets using a mobility prediction-based weighted clustering algorithm” [24] proposes an algorithm which is based on the WCA algorithm. In WCA, the overhead of Hello messages are high and hence to reduce this overhead, MPWCA was proposed. The duration between the Hello messages sent by the CHs is reduced. But, to maintain the link connectivity between the nodes and the CH at the time when there is no Hello message sent, MPWCA predicts the location of the CH. The previous locations of the associated CH are used by the ordinary node to predict the current location of the CH. Based on this prediction, the node is always aware of the current location of the CH and hence the network is connected or an action is taken if the node is isolated. Here, the prediction is applied by the nodes to remain connected to the clusters and hence MPWCA approach is classified as prediction applied during cluster maintenance.

In the MPBC scheme [26], the prediction of the time of stay is used for the cluster head election and cluster maintenance. Cluster formation is done by estimation of relative velocity among the nodes. The time of stay is calculated using the relative speed and the boundary of the coverage area. But in Stable clustering through mobility prediction [27], the probability of the stay of a mobile node in a particular cluster for certain duration is predicted. The prediction is done based on the Mobility trie formed using the past visits of the node to virtual clusters in the geographical area. It could be easily inferred that the mobility prediction is used in the cluster head election and cluster maintenance stages. The proposed scheme LET in [28] uses the location, direction, and velocity of two nodes to predict the time until the link between the two will stay. Similar prediction is done using the values of location, velocity, and acceleration over a while in the AR-1 approach. This prediction is used in the cluster maintenance stage.

In this paper, a stable clustering algorithm with probability of node lifetime is proposed. The approach uses key metrics of the node such as node degree, residual energy, trust worthiness of node and time of availability of node. The node having more trust and node with high probability of availability is selected as CH which helps in providing efficient and secure communication in the network. Trust of the node adds security to the communication and availability of the node provides stable clustering and reduces re-clustering cost.

3. Proposed Methodology

Clustering technique is proposed in this paper based on the weight calculation of the node by considering its prominent features. Nodes in the network have limited energy and node becomes CH consumes more energy compared to normal nodes. Energy is the one of the constraints of the node in MANET, which should be sustain for longer time. Due to mobility, providing stability to the network is a difficult task. Mobility is the key challenge in MANET which should be considered for maintaining the lifetime of the clustering [40]. Providing security to the network is another difficult task in MANET. Trust of the node is considered for providing security for the cluster. To guarantee efficient clustering, the proposed methodology use mobility prediction and predict the approximate time that the node stays within the area.

MANET is formed by nodes and communication links that can be represented by an undirected graph G(V, E) where V represents nodes in the network and E represents a set of communication links. The cardinality of V remains constant whereas cardinality of E varies from time to time with the creation and deletion of the communication links. All nodes are mobile in MANET. Nodes are free to move in the network in a random direction with random velocity. Each node has a transmission range Tx_{range} in which it can communicate with other nodes. Consider the transmission range for all the nodes is equal. And also consider all the nodes that deployed in the network are homogeneous.

Assumptions in proposed work:

- Assume network is formed into clusters randomly based on the location and density of the nodes.
- For each CH, the maximum number of neighboring nodes is limited to m for efficient MAC functionality. If it tries to support many nodes then the system functionality is degraded as nodes will wait longer for their turn to access resources. To avoid this problem the *degree of the node* is considered.
- A node consumes less energy to communicate with nearest neighbor nodes and consumes more energy for farther neighbor nodes, so the *distance with the neighbor nodes* is considered as another prominent feature.
- The *Battery* is one of the primary concerns in MANET. Nodes have very limited battery power. While electing CH residual energy consideration is important. If a node with less battery elected as CH, cluster will not be stable.
- Mobility is another concern in MANET. CH is selected such that it can stay in the cluster for a longer time. *Predicting the probability of* the node will stay in the cluster will help in maintaining stability.

Predicting the probability that a node stays in the cluster is one of the contributions in the proposed clustering methodology. This metric is one of the contribution in weight calculation to increase the lifetime of the cluster and maintain a stable CH [31]. The concept of mobility prediction of node in the network is inspired by Mobility prediction in MANET [20]. Authors predict the link failure using the mobility prediction of the node and find stable path. The idea is extended to find the probability a node can available and the time to which it is existed in a cluster.

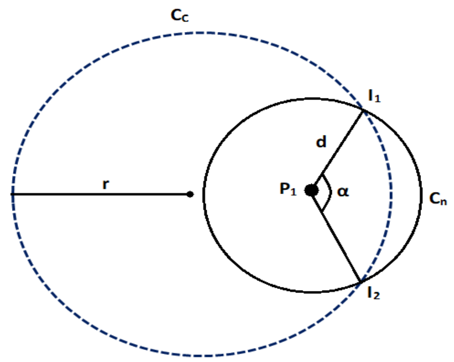

Figure 1. Probability of node n_1 stays in the cluster

Consider r is the radius of the cluster circle C_c and a node n_1 is at a position P_1 in the cluster as shown in Figure 1. To calculate the probability, the probability distribution function is used. Assume d is the distance that node has to travel to reach a point P_2. Now node n_1 can move in any direction to a distance d. Here density function helps in predicting node existence based on the direction. Node is free to move in any direction and forms a circle C_n with radius d. Find the center point of the circle C_c, consider it as (h,k). Center of circle C_n is position p_1(l,m).

The equation of the circles as:

$$(x-h)^2 + (y-k)^2 = r^2$$
$$(x-l)^2 + (y-m)^2 = d^2 \quad (1)$$

By using these equations, intersection points of the circle can be found. If two circles do not intersect, then the node stays in the cluster up to distance d irrespective of the direction of mobility. If two circles intersect at the points I_1 and I_2, the node will not stay in the cluster if it moves in the angle α that lies betweenI_1 and I_2. Let the angle of intersection be α.

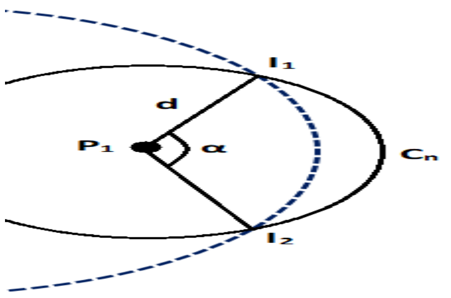

Figure 2: Angle of acceptance of node n1 in the cluster

In Figure 2, P_1, I_1 and I_2 as vertices, a triangle is formed. Now α can be found by using cosine rule. According to cosine rule square of the length of any side is equal to the sum of the squares of length of remaining sides minus twice their product and cosine of their included angle [37].

Probability of a node lies in the cluster is defined by:

$$P(d, P_1) = \frac{\beta}{\beta_{max}} \qquad (2)$$

where β is the acceptance angle and β_{max} is the maximum acceptance angle for the node to stay in the cluster.

If two circles do not intersect, 2π is the acceptance angle for a node to lie within the cluster. So β_{max} is 2π. β will be 2π-α with α as included angle at position P_1.

$$P(d, P_1) = \frac{2\pi - \alpha}{2\pi} \qquad (3)$$

To elect trustable node as a CH, Trustworthiness of the node is evaluated by considering different behavioral aspects. Each node is initially given behavioral value as 1. This is decreased later based on abnormal activities detected [29]. Nodes with behavioral level less than a threshold value will not be elected as CH even though; it has better characteristics like high energy, high degree or more. A similar metric is considered in Energy-efficient and safe weighted clustering algorithm [16]. Malicious node moves frequently in the network to attract other nodes for routing. The idea is not to elect a node which moves frequently in the cluster. Based on mobility, a node is categorized to normal or abnormal. An abnormal node may be a suspicious node or malicious node. Behavior Level (BL) [36] of the node i is defined based on considerations. BL_i is defined as:

$$\begin{aligned} &Normal\ Node: 0.8 < BL_i \le 1 \\ &Suspicious\ Node: 0.3 < BL_i \le 0.8 \\ &Malicious\ Node: 0 < BL_i \le 0.3 \end{aligned} \qquad (4)$$

The values of BL are categorized based on Trust management technique in [38] by R. A. Shaikh and Cluster based organizing algorithm in [39] by M. Lehsaini. . Along with considering mobility watchdog mechanism is included in trust computation. A node always observes its one-hop neighbors and suggests whether a neighbor node is reliable or not. If the node finds its neighbor node replicates, duplicates or changes the packets that it transmits or it does not transmit all the packets it receives then the node will triggers a failure and BL of the neighbor node is decreased by 0.1 units for an instance.

The distance between the node and its neighbors are considered to enhance the cluster stability. The sum of the distances D_n for each node with all its neighbors is calculated using (3)

$$D_n = \sum_{n' \epsilon N(n)}^{n} distance(n, n') < Tx_{range} \qquad (5)$$

As energy is the major constraint in MANET, battery of the node is to be considered. Battery of the node can be found by residual energy (Er_n) of the node at the time of the election.[11]

$$Er_{n_i} = E - (E_{Tx}(k, d) + E_{Rx}(k)) \qquad (6)$$

E is the energy that a node is currently having. E_{Tx}(k,d) refers to energy required by the node to transfer k bits to a distance of d with required amplifier E_a and is obtained by

$$E_{Tx}(k, d) = k.E_e + k.E_a.d^2 \qquad (7)$$

E_{Rx} (k) is the energy utilized by the node to receive k bits of data and is calculated by

$$E_{Rx}(k) = k.E_e \qquad (8)$$

Degree of the connectivity of the node is to be calculated to provide stable clustering. Find the neighbors (N(n)) of each node n, which gives the degree dg_n of n.

$$dg_n = N(n) = \sum_{n' \epsilon V, n' \neq n}^{n} distance(n, n') < Tx_{range} \qquad (9)$$

Weight (W_i) of a node n_i is calculated by using the equation (10)

$$W_i = w_1 P(d, P_1) + w_2 BL_i + w_3 D_n + w_4 Er_{n_i} + w_5 dg_n \qquad (10)$$

where the sum of coefficients is equal to 1 i.e., $w_1+w_2+w_3+w_4+w_5=1$.

The value of coefficient w_i varies based on the network topology and usage. If the network is concentrated on secure communication then the behavioral value of the node is given importance whereas if the network is for purely for fast communication then importance is given to mobility probability. The values of the coefficients in equation (10) will be chosen according to the priorities of the application in which the network is established.

3.1 Cluster Head Election

Electing a efficient CH is the main challenging task in clustering. Weight values will be calculated for each and every node in the network by equation (10) as discussed in above section. The node having highest weight value becomes CH. CH node broadcasts CH message to the neighbor nodes. After CH node advertises itself, neighbor nodes send join messages if they want to join to the cluster. CH replies with the acceptance message and make the node as cluster member (CM) to form a cluster as shown in Figure 3.

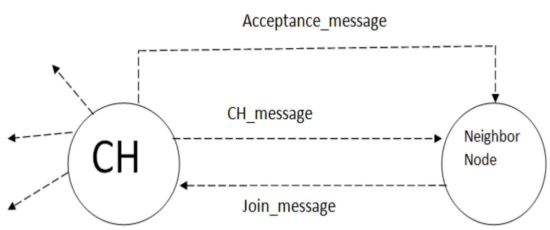

Figure 3: Cluster Formation

Algorithm:

1. Assign values to the coefficients of weight function w_1, w_2, w_3, w_4 and w_5.
2. For every node n_i
   a. Initially N(i)=0
   b. Find the list of neighbors by broadcasting neighbor message
3. Calculate the weights of all the nodes in the neighbor list using
   $$W_i = w_1 P(d, P_1) + w_2 BL_i + w_3 D_n + w_4 Er_{n_i} + w_5 dg_n$$
4. Initiate state vector of the node n_i
   Vector(ID, Cluster_ID, weight, neighbor nodes_list, size, state)
5. Initialize Cluster_ID= Null, Size=0 and State=Null
6. Repeat
   a. Any node n_i broadcasts Hello_message
   b. If N(i) >0 then
      i. Choose a node from neighbor list
      ii. Compare the weight of the nodes. The node having highest weight becomes CH. If both weights are equal then random node is elected as CH.
   c. Else node n_i is CH
   d. Update the state vector of the node n_i as Cluster_ID= CH_ID, Size=1 and state=CH
7. Newly elected CH broadcasts CH_message to its neighbors
8. For all, Neighnor nodes sends join_message to CH
9. If size of CH< Threshold_size then
   CH sends acceptance_message to the nodes
   Update the state vector as State= CM, Cluster_ID=CH_ID
   Increase the size of CH to 1

Else goto (6)

3.2 Cluster Maintenance

As discussed earlier election of CH is the prominent and challenging task in MANET to maintain stability in the network. As well, the cluster should be maintained and CH should react based on the dynamic structure of the cluster. Any node can enter or leave cluster at any time even CH can leave the cluster. In such cases cluster is maintained such as updating information about neighbor nodes and finding any misbehaving patterns of nodes and many.

3.2.1 Monitoring Cluster

If CH involves in monitoring nodes then its battery is consumed highly. To avoid this Second CH (SCH) is elected as a monitoring node. The node having the second-highest weight becomes SCH. It shares responsibilities of CH and reduces its battery usage. Intra cluster activities are done by SCH and inter-cluster activities are done by CH. SCH always monitors the battery level of CH if CH battery is less than the threshold (batterythreshold)then it informs CH to activate the process of delegation by sending Delegtionactive message and assign its responsibilities to SCH just before leaving in most of the cases. Meanwhile, SCH finds another SCH to start its delegation process. If a newly joined node in the cluster has more weight than SCH then CH delegation can be done to a newly joined node and SCH remains the same. Including a monitor node in the cluster reduces the communication cost of re-clustering and also increases the cluster stability as it shares responsibilities with CH in an efficient manner.

Algorithm:

1. CH elects the next weighted node as monitor node SCH
2. SCH monitors battery of CH
3. If (CH_battery < $battery_{threshold}$)
   CH ← SCH($Delegtion_{active}$)
4. If (SCH weight > all nodes in the cluster)
   CH makes SCH as CH
   Else
   CH makes the highest weight node as SCH
5. If (SCH is CH)
   SCH stars delegation process and elects next weighted node as SCH
   Else
   SCH remains same and updated its CH_ID

3.2.2 Detecting malicious behavior

A simple trust mechanism watchdog is used. Usually, CH observes all neighbor nodes and maintains the trust level. But in proposed algorithm SCA-NP, CH only observes SCH and often checks its behavior. If SCH shows any abnormal behavior, then CH removes SCH immediately and elects another node as SCH. SCH is responsible for observing remaining members in the cluster. SCH evaluates trust for remaining nodes and sends its trust value information to CH which uses the information at the time of routing. SCH uses watchdog mechanism and if it finds any node with abnormal behavior it sends id of the node to CH and informs CH to remove a node from the cluster. If SCH observes abnormal behavior with CH, then it starts re-clustering mechanism.

Algorithm:

1. Initially, CH observes SCH regarding its behavior
2. If CH detects abnormal behavior with SCH
   CH elects another SCH
3. CH assigns watchdog mechanism of other nodes to SCH
4. If SCH observes abnormal behavior of node i then
   SCH sends an alert message to CH as Misbehave(node_ID)
5. If CH gets misbehave alert from SCH
6. CH removes the node with node_ID from its routing table.
7. If SCH observes abnormal behavior with SCH it starts the re-clustering procedure

3.3 An Illustrative Example

The proposed clustering algorithm is demonstrated with figures in this section. 15 nodes are considered to execute the proposed scheme and obtained numerical values are tabulated in Table 1. All nodes in the network are homogeneous. Initially, all nodes have the same battery capacity but deduce based on their performance. Figure 4 shows the initial configuration of nodes that are placed randomly in the execution environment.

After installing nodes, the network is divided into clusters randomly based on the location and density of the nodes. The maximum number of nodes allowed in the cluster is limited to 5. The thick circle in Figure 5 shows the clusters formed in the network. Now clusters are available, a CH is to be selected based on proposed CH election algorithm

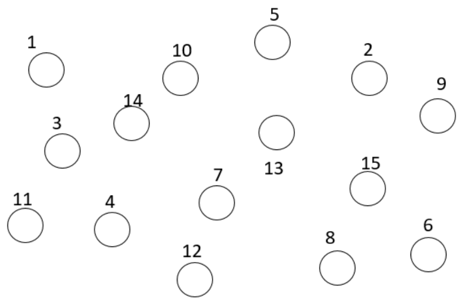

Figure 4: Initial configuration of nodes

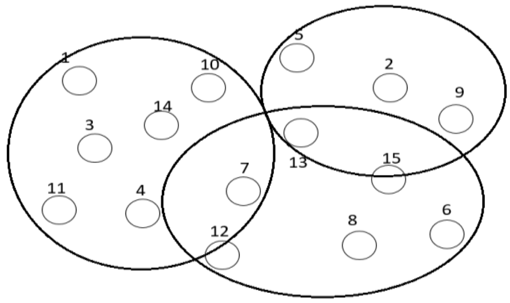

Figure 5: Cluster formation

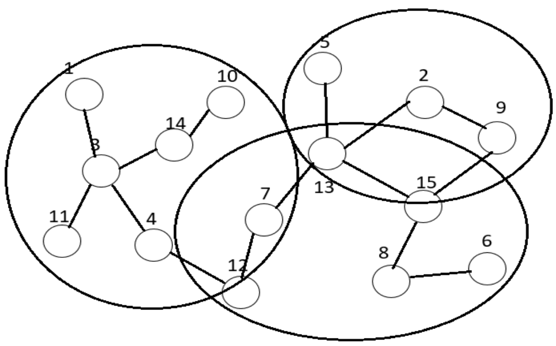

Figure 6: Finding neighbor nodes

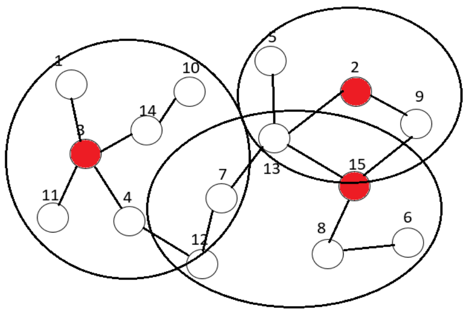

Figure 7: CH election

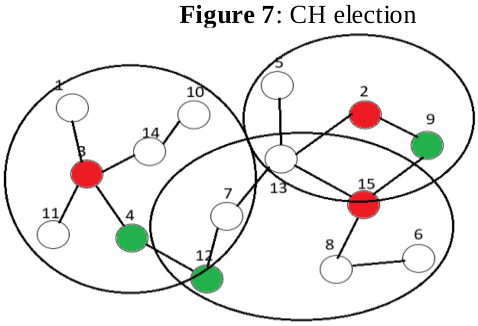

Figure 8: SCH election

Figure 6 shows the neighbor nodes for all the nodes. The link between two nodes represents the communication link. Through this communication link, it is possible to find an available degree of the node.

As discussed earlier, numerical values obtained from executing the proposed scheme listed in Table 1. The table includes the values of degree of the node (dg_n), Distance to neighbors (Dst_n), residual energy of the node (Er_n), the trust of the node (BLn), the probability that node stays in cluster (P(d, P1)) and weight (W_n) calculated. All the values are calculated using equations (1-6) discussed in 3.2. CH and SCH are elected based on obtained weights. A node having highest weight is elected as CH but before assigning CH to the node, consider BL value of the respective node and check whether it is malicious or not. If the node is malicious even though it has the highest weight, the next highest weighted node is elected as CH. FIG 7 and FIG 8 shows CH and SCH election using proposed scheme respectively.CH is represented with red color and SCH represented with green color nodes.

Table 1: Numerical values obtained from the proposed weight-based clustering scheme

Node_ID	dg_n	Dst_n	Er_n	BL_n	$P(d,P_1)$	W_n
1	1	4	3.2	0.4	0.6	1.84
2	2	8	3.5	0.6	0.7	2.89
3	3	11	2.9	0.8	0.8	3.48
4	2	7	3	0.7	0.3	2.5
5	1	4	2.8	0.9	0.2	1.79
6	1	3	2.6	0.5	0.8	1.61
7	2	7	3.3	0.1	0.7	2.49
8	2	7	3.6	0.5	0.9	2.74
9	2	7	2.8	0.8	0.5	2.55
10	1	2	2.9	0.6	0.9	1.53
11	1	2	3	0.9	0.8	1.43
12	2	8	3.4	0.4	0.6	2.78
13	3	15	2.8	0.3	0.7	4.13
14	2	4	2.9	0.7	0.4	1.91
15	2	8	3.5	0.8	0.6	2.92

While electing CH and SCH, malicious nodes can be identified easily by observing BL values. Nodes in malicious category removed from the network and new communication links are formed as shown in FIG 9.

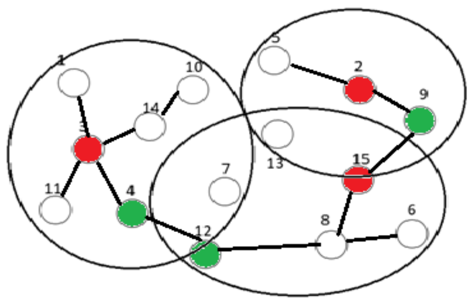

Figure 9: Removing malicious nodes

4. Simulation results and Discussion

Network with N number of nodes is simulated on a 500 X 500 meter square space using NS3. N varies from 10 to 100 and simulation is done with different velocities of the nodes and different transmission ranges. Nodes are configured randomly on the simulation space. All nodes are considered as homogeneous. Nodes are moving with the random velocity with a minimum velocity of 0 to maximum velocity 50. Maximum capacity of a CH to handle other nodes is considered as 10. 40 simulations have done to observe the accurate pattern of the nodes and to evaluate the performance of the proposed scheme. Transmission range varies from simulation to simulation. The battery power of the node is initially assigned for full and based on transmission rate it is reduced. The simulation parameters are given in Table 2.

Table 2: Simulation Parameters

Parameter	Meaning	Value
N	Number of nodes	10 to 100
X*Y	Network simulation Area	500 X 500
Tr_range	Transmission range of nodes	50 to 300
Velocity	Speed of the node	50-400 m/sec
Run time	Time of simulation	300 sec
CH_threshold	Maximum number of nodes a CH can handle	10

FIG 10 presents an average number of clusters formed for a number of nodes N varies from 10 to 100 with a transmission range of 200 m. The proposed scheme forms the same number of clusters when a network having 50 to 60 nodes. If the number of nodes increases, proposed algorithm forms less number of clusters. For 100 node number of clusters reduced from 8 to 6. If the network has more nodes proposed scheme forms a lesser number of clusters compared to existing ESWCA.

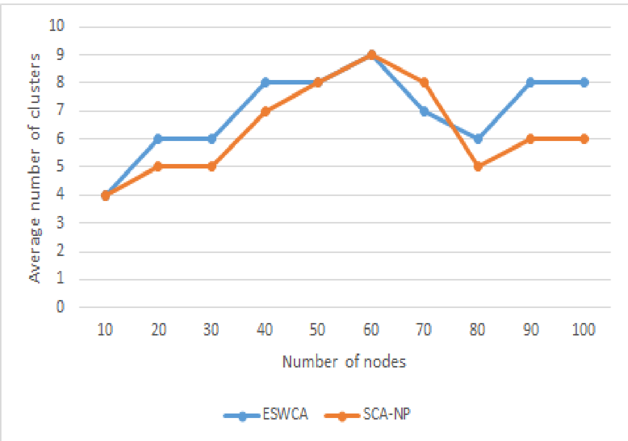

Figure 10: Average number of clusters formed for a number of nodes

FIG 11 depicts the average lifetime of the network with nodes varies from 10 to 100 using AODV protocol. It is observed that the network lifetime is not varying much when the nodes are more. There is a rapid change from 60 to 70 nodes. Network lifetime depends on the stability of the cluster and energy of the nodes. The proposed algorithm maintains the network for a long time because the algorithm distributed responsibilities of CH to two nodes CH and SCH. It avoids CH to exhaust or dead quickly.

FIG 12 depicts percentage of avoiding malicious nodes elected as CH. The proposed scheme is efficient than existing ESWCA because the proposed scheme not only considers BL of the node in weight calculation it also considers while electing CH. The proposed algorithm checks BL after finding the highest weighted node. If the node falls under malicious node it doesn't allow the respective node to become CH

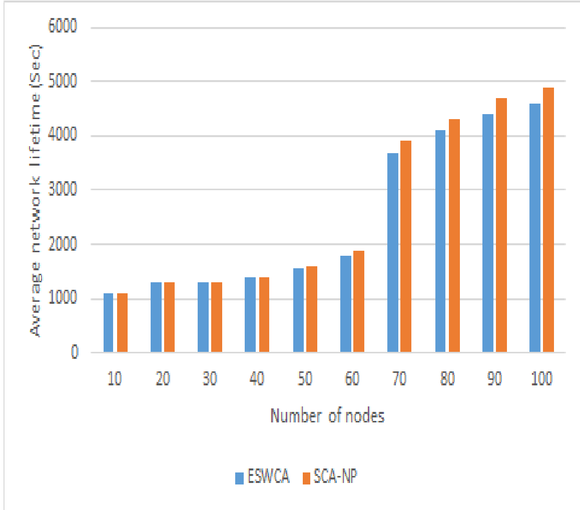

Figure 11: Average lifetime of the network to a number of nodes

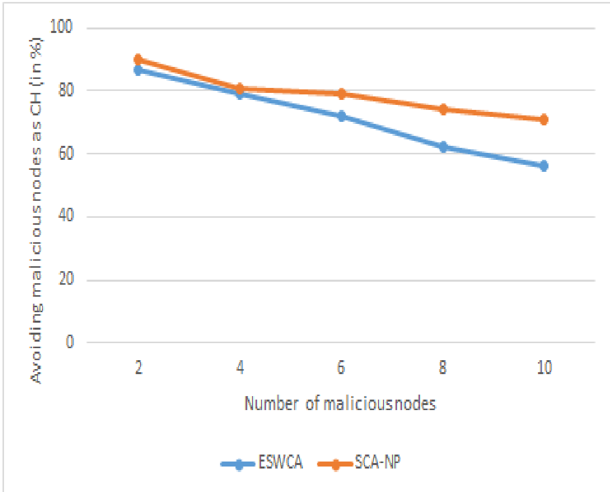

Figure 12: Percentage of avoiding malicious nodes as CH

FIG 13 presents the Packet Delivery Ratio (PDR) in the network. PDR is defined as the number of packets received by the receiver to the number of packets sent by the sender. As malicious nodes are increasing there is a decrease in PDR. Proposed algorithm SCA-NP proves its efficiency by avoiding malicious nodes as CH and also it detects malicious nodes and identify trustable nodes and sends data through them.

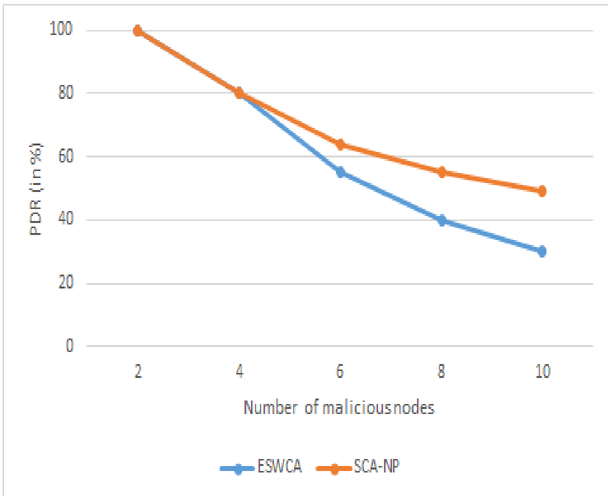

Figure 13: PDR for number of malicious nodes

5. Conclusion

SCA-NP is proposed in this paper to minimize frequent clustering procedure and to maintain network stability. The primary objective of the proposed scheme is to maintain stability along with security. To achieve this, weight-based clustering is chosen for electing efficient CH. For providing security in the network, every node is evaluated for its behavior and categorized to normal, suspicious and malicious nodes. Malicious nodes are strictly prohibited for CH election. Algorithm ignores the parameters of a node even though they are impressive when its BL is malicious. This algorithm not only avoids malicious nodes as CH it also helps in maintaining energy efficiency. In any Cluster, all the responsibility is taken by CH and it is solely responsible for maintaining a cluster. In the proposed scheme, a monitor node SCH is introduced which shares responsibilities of CH and helps to maintain cluster stability. As SCH shares responsibilities energy consumption of CH is reduced and helps in maintain network stability. Future work can be extended to increase PDR using link and mobility prediction to avoid re-routing frequently.

References

[1] M. Mauve, J. Widmer, and H. Hartenstein, “A survey on position-based routing in mobile ad hoc networks,” *IEEE Networks.*, vol. 15, no. 6, pp. 30–39, 2001

[2] Neeraj Garg, Sanjay K, Petros Nikopolitidis, J S Lather,“Eficient mobility prediction scheme for pervasive networks,” International Journal of Communication Systems, 2017

[3] V. S. Janani and M. S. K. Manikandan, “Efficient trust management with Bayesian- Evidence theorem to secure public key infrastructure-based mobile ad hoc networks,” Journal of Communications and Networking, 2018.

[4] E. Rehman, M. Sher, S. Hussnain, A. Naqvi, K. B. Khan, and K. Ullah, “Energy Efficient Secure Trust Based Clustering Algorithm for Mobile Wireless Sensor Network,” 2017.

[5] D. Zhao and D. Zhang, “A Distributed and Adaptive Trust Evaluation Algorithm for,” Q2SWINET, Nov 2016, Malta.

[6] A. Ben, C. Douss, R. Abassi, S. Guemara, and E. Fatmi, “A trust-based security environment in MANET : definition and performance evaluation,” *Ann. Telecommun.*, 2016.

[7] A. M. Shabut, M. S. Kaiser, K. P. Dahal, and W. Chen, “A Multidimensional Trust evaluation model for MANETs,” Journal of. Network and Computer. Applications, 2018.

[8] A. H. Networks, M. Chatterjee, S. K. Das, and D. Turgut, “WCA : A Weighted Clustering Algorithm for Mobile,” Cluster Computing, pp. 193–204, 2002.

[9] Yang Wei-dong,“Weight-Based Clustering Algorithm for Mobile Ad Hoc Network,” Cross strait Quad-Regional Radio Science and Wireless Technology Conference, pp. 787–791, 2011.

[10] P. Chatterjee, I. Sengupta, and S. K. Ghosh, “A Trust Based Clustering Framework for Securing Ad Hoc Networks,” ICISTM, Heidelberg, pp. 313–324, 2009.

[11] H. Zhou, “An Efficient Clustering Algorithm for MANET Based on Weighted Parameters,” International symposium on Computatonal ainttelligencce and Design, pp. 145–148, 2015.

[12] N. Karimi and M. Shayesteh, “An Innovative Clustering Method for MANET Based on,” International Journal of Computer Science and Telecommunications, vol. 3, no. 5, 2012.

[13] A. H. Hussein and A. O. A. Salem, “A Flexible Weighted Clustering Algorithm Based on Battery Power for Mobile Ad Hoc Networks,” International Symposium on Industrial Electronics, UK, pp. 2102–2107, 2008.

[14] S. Adabi and S. Jabbehdari, “SBCA : Score Based Clustering Algorithm for Mobile AD-hoc Networks,” The 9th International Conference for Young Computer Scientists, pp. 427–431, 2008.

[15] Z. Xing, F. Street, R. El, F. Street, and R. El, “A Robust Clustering Algorithm for Mobile Ad Hoc Networks A Robust Clustering Algorithm for Mobile Ad Hoc Networks,” Handbook of Research on Next generation networks and ubiquitous computing, December 2008.

[16] D. Amine, B. Nassreddine, and K. Bouabdellah, “Energy Efficient and Safe Weighted Clustering Algorithm for Mobile Wireless Sensor Networks,” *Procedia Computer. Sciencce*, vol. 34, pp. 63–70, 2014.

[17] Z. El-bazzal, M. Kadoch, B. L. Agba, F. Gagnon, and M. Bennani, “A Flexible Weight Based Clustering Algorithm in Mobile Ad hoc Networks,”International Conference on Systems and Networks Communications", Tahiti, 2006.

[18] S. B. Kulkarni, “ENB Cluster Head Selection Algorithm for MANET,” International Journal on Engineering Technology and Sciences, vol. 2,issue 0, pp. 4–6, 2015.

[19] R. Fernandes and R. Dsouza G.L, “A New Approach to Predict user Mobility Using Semantic Analysis and Machine Learning,” *Journal of Medical Systems- Mobile and Wireless Health*, vol. 41, issue 188, 2017.

[20] U. Palani, K. C. Suresh, and A. Nachiappan, “Mobility prediction in mobile ad hoc networks using eye of coverage approach,” *Cluster Computing*, vol. 2, 2018.

[21] Wenjila Li and Houbing Song, “ ART:Attack-Resistant Trust Management Scheme for Securing Ad Hoc Networks”, IEEE Transaction on Intelligent Transport Systems, Vol.17, Iss. 4, 2016.

[22] K. Wang and B. Li, “Group mobility and partition prediction in wireless ad-hoc networks,” in Communications, 2002. ICC 2002. IEEE International Conference on, vol. 2, 2002, pp. 1017–1021

[23] B. S. Mathapati, S. R. Patil, and V. Mytri, “Energy efficient cluster based mobility prediction for wireless sensor networks,” in Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on, March 2013, pp. 1099–1104.

[24] V. Bricard-Vieu and N. Mikou, “Qos in manets using a mobility prediction-based weighted clustering algorithm,” in Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob’2005), IEEE International Conference on, vol. 3, Aug 2005, pp. 390–396 Vol.3.

[25] V. Bricard-Vieu, N. Nasser, and N. Mikou, “A mobility predictionbased weighted clustering algorithm using local cluster-heads election for qos in manets,” in Wireless and Mobile Computing, Networking and Communications, 2006. (WiMob’2006). IEEE International Conference on, June 2006, pp. 24–30.

[26] M. Ni, Z. Zhong, and D. Zhao, “Mpbc: A mobility prediction-based clustering scheme for ad hoc networks,” Vehicular Technology, IEEE Transactions on, vol. 60, no. 9, pp. 4549–4559, Nov 2011.

[27] S. Sivavakeesar, G. Pavlou, and A. Liotta, “Stable clustering through mobility prediction for large-scale multihop intelligent ad hoc networks,” in Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE, vol. 3, March 2004, pp. 1488–1493 Vol.3.

[28] A. Venkateswaran, V. Sarangan, N. Gautam, and R. Acharya, “Impact of mobility prediction on the temporal stability of manet clustering algorithms,” in Proceedings of the 2Nd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, ser. PE-WASUN ’05. New York, NY, USA:

ACM, 2005, pp. 144–151. [Online]. Available: http: //doi.acm.org/10.1145/1089803.1089979
[29] Safa, H., Artail, H., Tabet, D, “A cluster-based trust-aware routing protocol for mobile ad hoc networks”, Wireless Netw. 16(4), 969–984 (Springer) (2010)
[30] Heinzelman,W.R.,Chandrakasan,A.,Balakrishnan, H, “Energy-efficientcommunicationprotocol for wireless microsensor networks”, In Proceedings of the 33rd Hawaii International Conference on System Sciences, Maui, HI, USA (2000)
[31] S.R.Drishya and Vaidehi.V, “Modified Energy Efficient Stable Clustering Algorithm for Mobile Ad Hoc networks” Advances in Intelligent systems and Computing 740, https://doi.org/10.1007/978-981-13-1280-9_42
[32] Bentaleb.A,Boubetra.A and Harous.S, “Survey of clustering schemes in mobile ad hoc networks”, Commun. Netw. 5(02), 8–14 (2013)
[33] Hurley-Smith.D, Wetherall.J and Andrew “SUPERMAN: Security using pre-existing routing for mobile ad hoc networks”, IEEE Trans. Mobile Computing. 16(10) (2017)
[34] Zabian. A, Ibrahim. A and Al-Kalani. F, “Dynamic head cluster election algorithm for clustered Ad-Hoc Networks”, Journal of Computer Science. 4(1), 19 (2008)
[35] Dhamodharavadhani. S, “A survey on clustering based routing protocols in mobile Ad Hoc Networks”, IEEE International Conference on Soft-Computing and Networks Security (ICSNS) (2015)
[36] S.R.Drishya and Vaidehi.V “Efficient Hybrid Scheme for Cluster Head Election in Mobile Ad Hoc Networks”, International Conference on Recent Trends in Advanced Computing (ICRTAC), Chennai, 2018
[37] T.Camp, J. Boleng and V. Davies, “A survey of mobility models for ad hoc network research”, Wireless communications on Mobile Computing, 2002
[38] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y. J. Song, “Trust management problem in distributed wireless sensor networks,” in *Proceedings of the 12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA '06)*, pp. 411–414, August 2006.
[39] M. Lehsaini, H. Guvvennet and M. Feham, “An efficient cluster based self organization algorithm for wireless sensor networks”, International Journal of Sensor Networks, vol 7, no. 1-2, pp 85-94, 2010
[40] Kalpana Murugan, AI-Sakib Khan Pathan, “A routing algorithm for extending mobile sensor network’s lifetime using connectivity and target coverage”, International Journal of Communication Networks and Information Security (IJCNIS), Vol 11, No 2, 2019