Mobility Aware Voronoi Hexagonal Clustering Scheme with Trust for Securing Mobile Ad-Hoc Networks

JANANI.V.S AND M.S.K.MANIKANDAN
Department of ECE,
Thiagarajar College of Engineering, Madurai-15,
INDIA
jananivs@tce.edu

Abstract: Mobile Ad-hoc Networks (MANET) are susceptible to several attacks due to the salient characteristics of mobile nodes. However, the major challenge to ensure secures network functionality. Trust has been recently recommended as an effective mechanism to meet this challenge. In this paper, we propose and analyze mobility aware distributed trust based hexagonal clustering scheme (HTMAC) to secure MANETs. In contrast to the existing clustering techniques, we present a distributed hexagonal clustering model with Voronoi technique where trust accomplished. To increase the spatial reuse, the network areas are clustered into congruent hexagons with Voronoi geometric features. Each node in the proposed scheme computes the trustworthiness of to enhance the security. For scalability and dynamic reconfigurability, we consider a cluster-based approach by which nodes are broken into subgroups. Headers in the clusters securely communicate with each other to agree on a network functionalities and node mobility-instigated events. Relevant simulation results demonstrate that our clustering model is efficient to guarantee a secured and mobility-adaptive ad-hoc network with trustworthy mobile nodes.

Key words: Trust, Voronoi, Hexagonal Clustering, MANET, Mobility, Security.

1 Introduction

An ad-hoc network offers unrestricted mobility with the lack of any predefined infrastructure. This paradigm of network forms a multi-hop framework of independent nodes, without any centralized maintenance. Unlike any fixed network, the autonomous nodes in MANET are liable to attacks ranging from passive to active, due to the dynamic topology. Due to this characteristic of mobile nodes, it is difficult to provide a centralized static security solution. This is because; single point failure of the system fails the entire network functionality. Hence a distributed security solution that can adapt the unique nature of MANET should regulate. Moreover, security solution can be more sensible to provide security services and to revoke attackers. Trust, in recent years, is considered as a critical aspect in the design of a secure distributed system. The nodes in the network setup a trust relationship among themselves by evaluating the trust value. In this paper we present such a distributed security solution that quantifies nodes behaviour in the form of trust. Clustering, an antecedent in network classification supports the proposed scheme to reduce the overhead while analyzing the network as a whole. Here, the network is divided into interconnected groups called clusters and a co-ordinator for each group called clusterhead. The clustering process allows better performance of the protocol by improving the spatial reuse, scalablity, throughput and power consumption. Besides, this network structuring reduces the energy consumption as well as communication bandwidth in MANET. Unlike the conventional circular shape of clustering, we present a hexagonal shape, which closely approximates the circular patterns to partition an adjacent and non-overlapping group of nodes. This paper is structured as follows. In Section 2, the works related to clustering in MANET are described. Section 3 describes the proposed clustering technique with cluster formation and header section. Section 4 presents the mobility adaptive clustering model followed by the system model in Section 5. The performance evaluation and simulations is illustrated in Section 6 and the concluding remarks appear in Section 7.

2 Related Work

On recent years researchers focus on MANET security issues. It is difficult to provide a complete security solution to mobile networks due to its wireless connectivity, dynamic topology and infrastructure-less features. Mobility of nodes is the prominent factor that affects the topology and routing issues. To cope with the dynamic nodes, clustering techniques has been widely applied in MANET with respect to the mobility factor. Many clustering algorithms [1, 2] has long been studied and applied in MANET from decades. A stable clustering model with mobility behaviour was presented in [3]. In [4] Ni et al presented a mobility prediction based clustering model for highly mobile nodes, wherein the relative speed of each node was estimated. A location and relative mobility speed based algorithm for cluster head selection was introduced in [5]. In MOBIC [5] the cluster construction and header selection considered mobility as the critical decision criteria. To increase the bandwidth reuse, the network areas are clustered into congruent polygons security features. A hexagonal geometric distribution of nodes was introduced by Y.Z. Huang [6]. This partitioning technique has shown to increase the network capacity and throughput of the network. It was proven the regular hexagons have flexibility to be partitioned into smaller hexagonal shapes and grouped together to form larger ones. Withal, these clustering models increases the control overhead of cluster construction, maintenance and cluster head selection. Nevertheless, there are certain flaws in the existing MANET clustering schemes where the nodes are assumed to be co-operative. Owing to the presence of topology, providing a promising security to the mobile nodes in MANET is difficult to achieve. As an effective mechanism to consider issues in node cooperation and security, trust has been highly recommended in recent researches. J.Hung and D.Nicol [7] quantified trust relationships with the risk in a PKI system. A fully trust based PKI approach for adhoc networks was presented in [8-11]. This approach proved to eliminate security vulnerabilities to a large extend with maximized performance characteristics. In this paper we employ a trust based clustering scheme to secure MANET and to make the network flexible for dynamic mobility.

3 Proposed Clustering Methodology

This section describes the distributed trust based clustering framework to adapt the active topology and to secure MANET. An efficient clustering scheme is designed with the ad hoc environment to form stable clusters for the underlying network operations. To adapt the dynamic mobility of MANET, the diameter of the cluster should be flexible and so herein, we use hexagonal shape non-overlapping clusters. In the proposed scheme, each cluster has exactly one cluster head (CH) elected based on trust value, that is one hop distant from all the cluster members, as shown in Fig 1. The nodes in the boundary region and within the transmission range of any two CH are considered as gateway nodes, which handles cluster-to-cluster operations. The CH monitors its neighbour nodes with their trustworthiness, within each cluster. We assume all the nodes communicate through bi-directional channels so that each node can forward as well as hear from its neighbouring nodes.In an ad hoc Uncertain Clustering (UC) model, it has been assumed that a node $'n_i'$ should be located inside a region with a Probability Density Function (PDF) to describe the distribution of nodes within a region. To compute the closeness of the node and the cluster representative, different methods based on mean, Euclidean distance and probability have been in practice. However**,** these traditional clustering techniques of uncertain nodes increase the computational complexities and communication cost in mobile environment, especially in mobile ad-hoc networks. To construct a highly desirable uncertain clustering cell in MANET, we propose to use Voronoi diagrams (VD) based clustering in which the clustering issues are managed considering the drawbacks of existing DC methods. Voronoi diagrams are applied for wireless application as proposed by Fan et al in [12] and Kao.B et al in [13]. Stojmenovic .I et al in [14] introduced a distributed algorithm to compute the Voronoi region of each node. To increase the spatial reuse, the network areas are clustered into congruent polygons with Voronoi geometric features. A hexagonal spatial geometric distribution of nodes was introduced by Zhuang.Y et al in [15]. This partitioning technique has shown to increase the network capacity and throughput of the network. It was proven the regular hexagons have flexibility to be partitioned into smaller hexagonal shapes and grouped together to form larger ones.

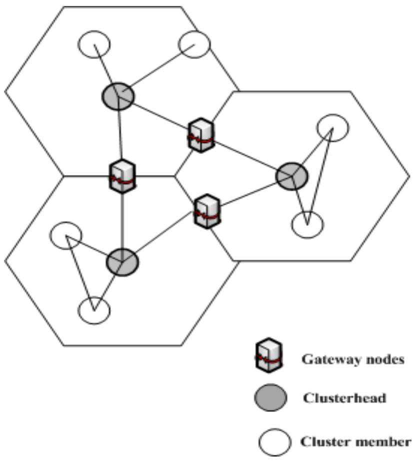


Figure 1: Hexagonal Clustering

In MANET, VD is used to partition network into clusters based on Euclidean distances to nodes in a specific subset of the plane. A Voronoi diagram represents the region of influence around each of a given set of nodes. This geometric structure partitions the entire plane into polygon cells, called Voronoi polygons, formed with respect to n nodes in a plane. In recent years this structuring concept is widely used for exploring location and routing based issues. The Voronoi partition or cluster for a given set of nodes is unique and produces polygons which are route connected. A Voronoi polygon, traditionally, constructed as follows

$$V_{(n_i)} = \left\{y \middle| d(n_i, y) \leq d\,(n_j, y); i \neq j\right\} \qquad (1)$$

where $V_{(n_i)}$: Voronoi polygon of n_i

n_i : Node and y : Set of points closer to n_i

$d(n_i, y)$: Distance from point y and n_i and

(n_j, y) : Distance from point y and n_j.

3.1 Cluster Construction

In the first step Voronoi clusters (VC) are constructed on a set of nodes $N = \{n_1, n_2 .... n_k\}$ with a distance function $d: S^m \times S^m \rightarrow S$ (m-dimensional space) giving the distance $d(x, y) \geq 0$ between any nodes $x, y \in S^m$.The VD partitions the space S^m in k cells with cluster representatives $C = \{c_1, c_2 \dots \dots . c_k\}$ with the property as:

$$d(x, c_i) < d(x, c_j) \forall\, x \in V(c_i), c_i \neq c_j \qquad (2)$$

In the second step the distance between the nodes and a cluster node is calculated. The Voronoi partitioning of a network can be of any polygonal shape and for its beneficial geometrical characteristics, we assume that the uncertainty region of N_i is a regular hexagon with nodes whose centre are equidistance to each other with distance d and radius r, where $r > 0$.The hexagonal clustering partitions a larger area into adjacent, non-overlapping areas and can be subdivided into smaller hexagons. Nodes joins to form hexagonal clusters and each cluster consists of CH and Cluster Members (CM) as shown in Fig 1.The distance $d(a, b)$ between nodes in MANET plays an important role in determining the network performance. We shall assume that the nodes of the ad-hoc network are independent and randomly distributed in the hexagonal structure. The edges of the hexagonal polygon is perpendicular to the line joining a node with another in N. Considering the radius, for any query point $\in S$, (2) can be written as:

$$d(p, c_i) - d(p, c_j) = r_i + r_j \qquad (3)$$

If two nodes overlap, the distance $d(n_i, n_j) < r_i + r_j$ and (3) become unreal, which means the edges cannot be found and we consider the cluster as empty. The hexagonal cluster construction in the MANET is illustrated in Algorithm 1.

Algorithm 1: Proposed Cluster Construction

```
Input: Nodes $N = \{n_1, n_2 \dots \dots \dots \dots n_k\}$
Output: Clusters $C = \{C_1, C_2 \dots \dots \dots \dots C_k\}$
1. for each $n_n \in N$ do ;
2. The VD for cluster construction consider an expected region of node $n_i$ and the neighbouring region of VC edge $E_n(m)$ . The expected region of $n_i$, denoted by $E_{r_i}$is the intersection of all the internal regions. ie.,
       $E_{r_i} = \bigcap_{j=1.....|E| \wedge j \neq i} \overline{X_n(m)}$        (4)
   where the neighbouring region, $X_n(m)$ is the region on one side of the cluster cell edge $E_n(m)$ and $|E|$ is the empty set.
3. $E_{r_i} \leftarrow S^m$        ; initialize expected region
4. for each $n_m \in N \wedge m \neq n$, do
5. The clustering polygon can be generated by excluding all the neighbouring regions from the domain space. The overlapped regions are reduced to generate the expected region $E_{r_i}$.
```

```
6.  $E_n(m) \leftarrow$ VC edge of $n_n$
                              ; compute edge of Voronoi cluster
7.  $N_n(m) \leftarrow$ neighbour of $E_n(m)$
                    ;compute the neighbour
8.  $E_{r_i} \leftarrow E_{r_i} - N_n(m)$
        ;reduce overlap
9.  end for
10. For each node $n_j$, we verify the expected region lie inside a Minimum and Maximum Region Bounding (MinMax-RB) of the domain space.
11. if $E_{r_i} \subseteq$ MinMaxRB, do
12. Let us consider six equilateral triangles in a regular hexagon. For calculation we take a single equilateral triangle $\Delta OAF$. A circle with centre $c_n$ and radius $r_n$ is assumed to intersect the $\Delta OAF$.
13. $C_n \leftarrow E_{r_i}$
                    ;assign expected region as cluster
14. Considered as neighbouring regions $N_n(m)$ and the region where the area of the circle and the neighbouring region overlap as overlap region $O_i$( ie., $O_i(x,y) = O_1 + O_2 + O_3$ ).
15. Calculate probability of the expected region $E_{r_i}$ in a hexagonal cluster with area $A$ and $(x,y)$ as co-ordinates of any random node is given as

    $P_{E_{r_i}} = \frac{1}{A^2} \iint \left[\pi {r_n}^2 - \sum_{i=1}^{6} O_i(x,y)\right] dx\, dy$   (5)

    $P_{E_{r_i}} = \frac{\pi {r_n}^2}{A} - \frac{6}{A^2} \iint O_i(x,y) dxdy$   (6)
16.     end if
17.     end for.
```

3.2 Cluster Head Selection

In MANET, the nods join or leave the cluster dynamically and thus the CH selection is difficult .We consider a distributed cluster head selection procedure with n nodes, which are of h hops distance within a cluster. It is much easier to select an efficient mechanism to establish security, if trust relationship among the nodes is obtainable for every cooperating node. Hence to provide a secured communication amongst cooperative nodes, it is important to calculate the trust and distrust degrees of nodes in the network. The trust of a node can be defined as the probability of belief of a trustor (t) on a trustee (s), varying from 0 (complete distrust) to 1 (complete trust). The probability of trust and distrust of the trustor on information (i) send by the trustee with context to belief (b) is given in the (7) and (8) [16] :

$$Trust\ Degree, TD(t,s,i,b) = P[belief\ (t,i) | made\ By(i,s,b) \wedge beTrue(b)\ ] \quad (7)$$

$$Distrust\ Degree, DTD(t,s,i,b) = P[belief\ (t, \neg i) | made\ By(i,s,b) \wedge beTrue(b)\ ] \quad (8)$$

In order to measure the trust degree explicitly in an ad-hoc environment, we present a trust calculation method with uncertainty degree. With this a high level of trust can be achieved for secured communication. The certainty of nodes in MANET is considered as the summation of trust and distrust degrees. Consequently, thus the uncertainty degree (UD) is defined as

$$UD(t,s,i,b) = 1 - certainity\ of\ nodes \quad (9)$$

An important factor that affect the trust level of a node is the Encounter History (EH), which specifies the number of successive interactions between the trustor and the trustee in a network. Initially we assume EH as greater than or equal to 0. The trust and the distrust level of any node can be measured with the relation as shown in (10) and (11).

$$TD(t,s,i,b) = \frac{\sum_{x=1}^{n} e_p\ (x)}{EH} \quad (10)$$

$$DTD(t,s,i,b) = \frac{\sum_{x=1}^{n} e_n\ (x)}{EH} \quad (11)$$

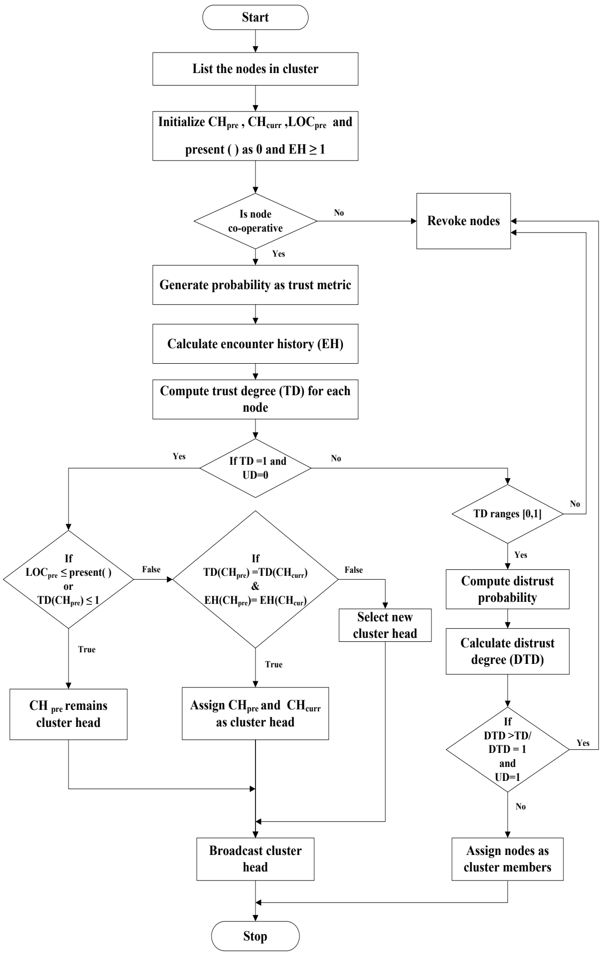
Therefore (9) $\Longrightarrow$

$$UD(t,s,i,b) = 1 - \left[\frac{\sum_{x=1}^{n} e_p\ (x)}{EH} + \frac{\sum_{x=1}^{n} e_n\ (x)}{EH}\right] \quad (12)$$

The degree of successive encounter $'x'$ made be trustee on trustor may either be positive (represented as $e_p(x)$) or negative (represented as $e_p(x)$). Here, to evaluate the trust, we consider three cases of uncertainty degree i.e, $= 0$, $0 < UD < 1$ and $UD = 1$. When the uncertain degree is low $(UD = 0)$, the nodes are highly trustable. This highly certain case shows that the trustor is very much confident with the trustee. If the uncertain degree varies from low to high $(0 < UD < 1)$, the trustor may not have sufficient confidence with the trustee. On the other hand a highly uncertain case occurs when the uncertain degree $UD = 1$. At this state the trustor may be completely unknown about the trustee.

The nodes with highest trust degree. ie., $UD = 0$ and $TD = 1$, is considered as CH, initially at time T_1. As time progresses, the topology changes frequently in a MANET that varies the cluster nodes and the cluster heads. Hence the cluster head selection procedure is adaptable for the change in topology. The trust value of each node is recomputed and the CH is selected, comparing the current CH (CH_{curr}) with the previous CH (CH_{pre}) and location (LOC_{pre}).

The nodes with trust degree between 0 and $1(ie.,0 < UD < 1)$ are undergone distrust test to reduce the rate of risks. On comparison with the trust degree and the distrust degree of such nodes, they are either revoked or considered as cluster members ie., the nodes with highest distrust degree $(DTD = 1 \; or \; DTD > TD \; and \; UD = 1)$ are revoked and the remaining nods are assigned as CH. This trust based cluster head selection eliminates a certain amount of risk in communication within the network. The detailed cluster head selection process is shown in the flow chart 1.


Start
List the nodes in cluster
Initialize CH$_{pre}$, CH$_{curr}$,LOC$_{pre}$ and present ( ) as 0 and EH ≥ 1
Is node co-operative
No
Yes
Revoke nodes
Generate probability as trust metric
Calculate encounter history (EH)
Compute trust degree (TD) for each node
Yes
If TD =1 and UD=0
No
TD ranges [0,1]
No
Yes
If LOC$_{pre}$ ≤ present( ) or TD(CH$_{pre}$) ≤ 1
False
If TD(CH$_{pre}$) =TD(CH$_{curr}$) & EH(CH$_{pre}$)= EH(CH$_{cur}$)
False
Select new cluster head
Compute distrust probability
Calculate distrust degree (DTD)
True
True
CH $_{pre}$ remains cluster head
Assign CH$_{pre}$ and CH$_{curr}$ as cluster head
If DTD >TD/ DTD = 1 and UD=1
Yes
No
Broadcast cluster head
Assign nodes as cluster members
Stop

Flow chart 1: Trust Based Cluster Head Selection Process

To perceive the exact location information of any node, each node in the network is enabled with a position identification system. Our proposed scheme makes use of the clusters as well as the location information intensively.

4 Mobility Adaptive Clusters

The proposed clustering scheme is designed to achieve a stable cluster organization with minimum communication overhead and complexities, in the presence of dynamic node mobility. This is established by two processes namely $Node \; Registration$ and $Node \; Resign$,as described below.

4.1 Node Registration

When a node attempts to join a cluster, it should be registered with the other nodes, especially in an unstable topological ad hoc network. The registration procedure is described in Algorithm 2.

Algorithm 2: Node Registration

1. As shown in Fig 2, $\boldsymbol{CH}$ broadcasts an $\boldsymbol{CLUSTER\_ACTIVE}$ beacon to update the status of the existing cluster members as well as to make feasible the cluster for new nodes $'n'$to join.
2. At regular intervals, the nodes that sense the $\boldsymbol{CLUSTER\_ACTIVE}$ beacon sends a $\boldsymbol{ACTIVE}$ message which includes $\boldsymbol{S_{id}}$,$\boldsymbol{T_f}$ and $\boldsymbol{NLI}$.
3. The $\boldsymbol{CH}$ verifies each $\boldsymbol{ACTIVE}$ message to validate the trust and location of the $\boldsymbol{CM}$.
4. When a new node attempts to join the cluster, it sends $\boldsymbol{REG\_CLUSTER}$ message to the $\boldsymbol{CH}$, which includes $\boldsymbol{S_{id}}$,$\boldsymbol{T_f}$ and $\boldsymbol{NLI}$ of the node n.
5. After verifying the T_f and location history , if the $\boldsymbol{CH}$ finds the node n as trustable, it sends a $\boldsymbol{TEMP\_ \; JOIN}$ message to temporarily join the cluster.
6. $\boldsymbol{CH}$ broadcasts a $\boldsymbol{VOTE}$ message along with the status of newly joined node to all its members, for calculating the $\boldsymbol{NTV}$ for the node n.

7. After a review period, $\boldsymbol{CH}$ calculates the $\boldsymbol{T_{rate}}$ of the node n ,with the experiences got from the voters.
8. If the $\boldsymbol{T_{rate}}$ is higher than the $\boldsymbol{T_t}$ set by the $\boldsymbol{CH}$, it sends a $\boldsymbol{TC}$ to the node n to confirm the temporary registration.The status of is node n is broadcast to all the members by the $\boldsymbol{CH}$.

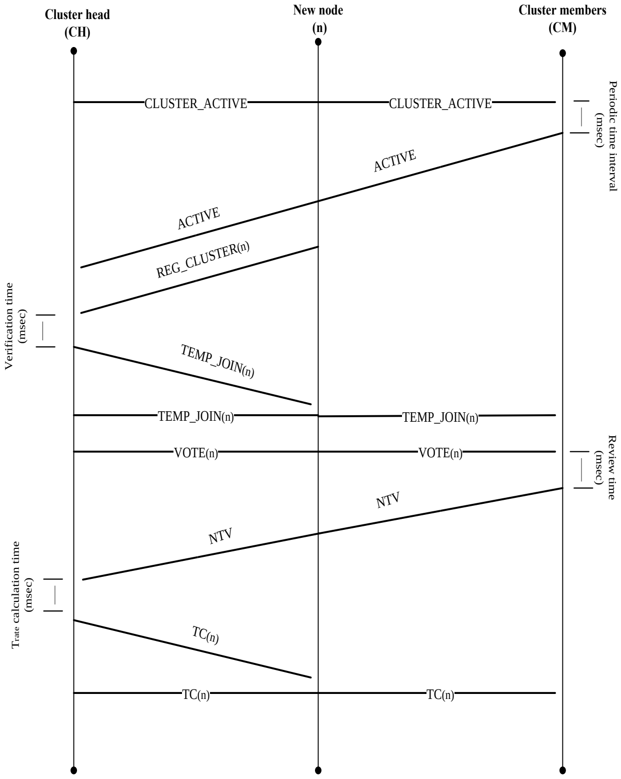


Figure 2: Node registration in a cluster

4.2 Node Resignation

The nodes get deactivated from a cluster due to certain reasons; connection failure, cluster disconnection or self departure. If a node voluntarily departs from the cluster, it announces its resignation by broadcasting a $RESIGN$ message to all the nodes before leaving the cluster.At periodic interval, each node in a cluster has to send a $ACTIVE$ message in response to the $CLUSTER\_ACTIVE$ message broadcast by the CH. When the CH doesn't receive $ACTIVE$ message from any node for certain waiting time (say t_w), the CH broadcasts a $SENSE$ message to all its members. For example, if the silent node is node m, CH sends $SENSE_m$ to the members. The cluster members who senses the presence of the deactivated node either due to connection failure or cluster disconnection, sends a $DETECT$message to the CH.The CH verifies the $DETECT$ message and tries to establish a connection with the silent node ans asks for its $ACTIVE$ message.The CH ratify the node m if the node replies or instead, CH assumes node m as damaged and broadcast a $RESIGN_m$ message to all the members.

5 System Model

5.1 Cluster Model

In the proposed clustering method, we divide the entire operational region into different equi-sized hexagonal clusters of area $A = \pi r^2$,where r is the radius of the cluster region.The number of hexagonal clusters in a region is given by

$$N_c = 3\text{ɗ}^2 + 3\text{ɗ} + 1 \qquad (13)$$

where ɗ is the degree of rings. The N_c value is obtained from the mathematical induction in the network coverage model used.For example, in Fig 3 the total number of clusters $'N_c'$ is 7 with degree of rings surrounded 'ɗ' =1.

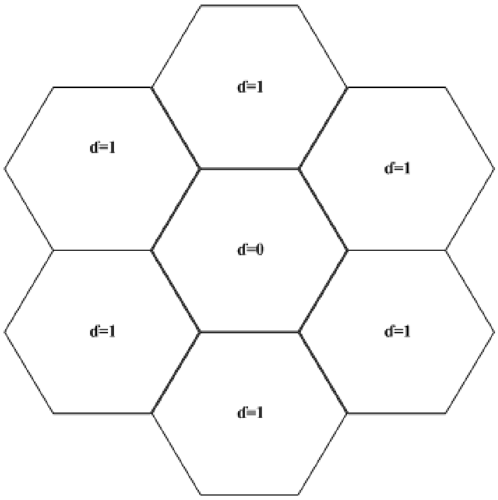


Figure 3: Network region with N_c is 7 and $\text{ɗ} = 1$.

We assume the random nodes are distributed in a homogeneous passion fashion of density d_p, over the hexagonally clustered network region of area A. The average number of nodes (Ɲ) in any cluster depends on the area of the cluster and the density of distribution, which is given as

$$\text{Ɲ} = \pi r^2 d_p \qquad (14)$$

Assume the rate of node joining the cluster be λ_j and the rate of node resigning from the cluster be λ_r. Therfore, the probability that a node is registered in a cluster can be ${}^{\lambda_j}\big/_{(\lambda_j + \lambda_r)}$ and the probability that it is resigined from a cluster is ${}^{\lambda_r}\big/_{(\lambda_j + \lambda_r)}$. In a hexagonal cluster region, the average number of active nodes is given as ${}^{\text{Ɲ}\lambda_j}\big/_{(\lambda_j + \lambda_r)}$. Moreover, the rate of all nodes registered in any cluster be R_j and the rate of all nodes resigned from the cluster be R_r, given as

$$R_j = \lambda_j * \text{Ɲ} * {}^{\lambda_r}\big/_{(\lambda_j + \lambda_r)} \tag{15}$$

$$R_r = \lambda_r * \text{Ɲ} * {}^{\lambda_j}\big/_{(\lambda_j + \lambda_r)} \tag{16}$$

In the mobility adaptive cluster, the nodes can move dynamically within a cluster and across the boundary region. Let μ be the rate of mobility of a node when there is one cluster and μ_m be the mobility rate of the node for N_c clusters. Then, the mobility rate across the boundary is given by

$$\mu_m = (2\text{ɗ} + 1)\mu * \text{Ƙ} \tag{17}$$

where, factor Ƙ represents the intra-cluster mobility of the nodes for whom the mobility across the boundary is not applicable.

5.2 Security Model

The proposed clustering model provides assurance for security using hard security and soft security approaches using trust, as mentioned below.

- Authentication: When a node joins a cluster, the node's identity is authenticated based on the trust function. *Source authentication* is ensured during the verification process and TC is signed to authenticate the source node. *Location authentication* is performed by authenticating the NLI, especially in a mobile network like MANET.
- Integrity: To preserve the integrity, a node calculates its T_{rate} with the positive responses it obtained during cluster construction.
  - Access control: The unauthorized use of resources is prevented using trust within each cluster. The services and resources allocated to the network are accessed by trustable node alone in the proposed cluster model.
- Communication risk: The proposed system indicates the presence of untrustworthy nodes that dissimate false communication. The CH validates each of its member's trust with T_t, below which it presumes certain communication risks and revoke those dishonest nodes from further cluster applications.
- Cluster availability: A $CLUSTER\_ACTIVE$ beacon at regular intervals make the cluster to work promptly so that no service denial for trustworthy nodes is assured.

5.3 Attack Model

We consider certain attacks in MANET as follows.

- *Dropping attack* interrupts the service availability of the nodes. The attackers deactivate nodes from their cluster by making a connection failure or cluster disconnection. The $SENSE$ beacon send by the CH during node missing, re-establishes the connection with the deactivated node, after verification processes.
- *Fake recommendation attack* falsely sends recommendations to include an untrustworthy node in the cluster functionalities. The trust calculation we used provides importance for analyzing the trustworthiness of any node, which degrades fake recommendations.
- *Sybil attack* can break down the security, when a node in the network claims multiple identities. The integrity check of the node gets rid of such attackers, where the honesty of that node is proved. Also the NLI records the location history of each node, which aids the CH to detect the attacker node with multiple identities and same location particulars.
- *Impersonation attack* can be an identity spoofing, node cloning, reply or an unauthorized access. However, the attackers fail to pass the source and location authentication as well as integrity check.

6 Simulation Results

In this section, a simulation environment is developed to evaluate the performance of the proposed HTMAC scheme against CBRP [17], 2ACK [18], and CBTRP [19]. The simulation model shows the efficiency of clustering algorithm in term of cluster's crucial properties namely mobility adaptiveness, effectiveness in stability and efficiency of HTMAC algorithm.

6.1 Mobility adaptiveness

To show the efficient adaptiveness to the mobility property of HTMAC scheme, we considered two inherent properties of cluster: size of the cluster and probability of node in a cluster. Fig 4 and 5 shows the mean cluster size and the probability of node in a cluster with the velocity of node respectively. The mean cluster size represents the number of nodes in the cluster with mobility as in Fig 4. The simulation result shows the desirable characteristic of HTMAC to adapt mobility. HTMAC scheme maintains larger number of nodes for lower mobility while decreasing the number of nodes for higher mobility.

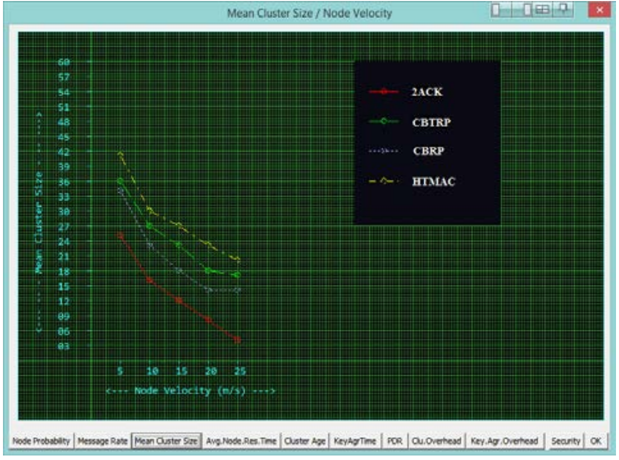


Figure 4: Mean cluster size with node velocity

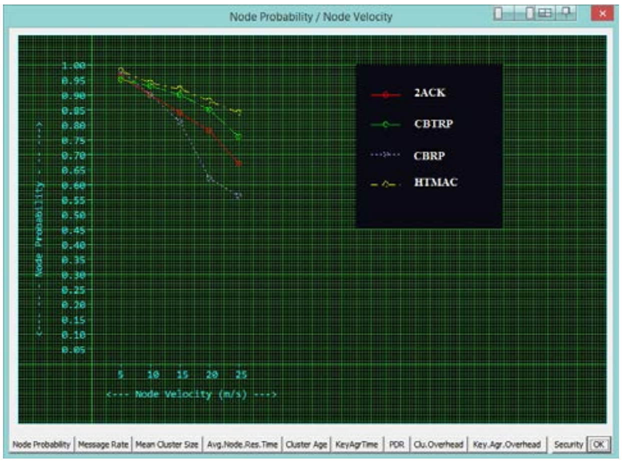


Figure 5: Node probability

Fig 5 shows the probability of node in a cluster with the effect of mobility. The results shows the nodes remain in any cluster with higher probability at larger mobility. The probability of a node remain clustered is greater than 0.85 even for highest node velocity.

6.2 Effectiveness in stability

The stability of HTMAC scheme is measured in terms of node residence time and cluster age. Fig 6 represents the time each node survive in a cluster, know as residence time, with respect to the node velocity. The node residence time varies with the probability of node in the cluster. The average survival time drops to 15mts when the node velocity reaches 25m/s as shown in the Fig 6. This is due to the lower rate of probability of nodes being clustered.

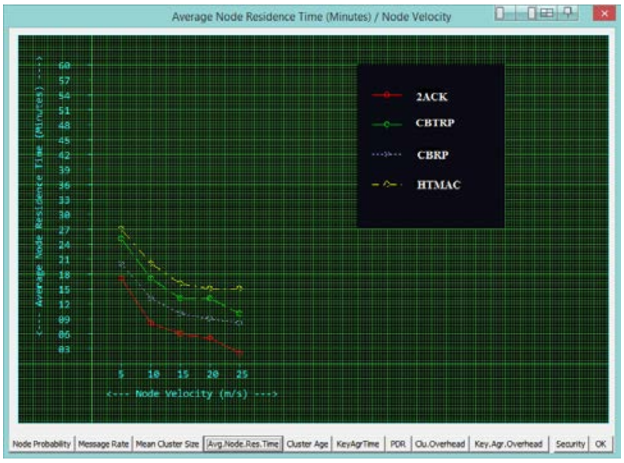


Figure 6: Average node residence time with node velocity

Fig 7 demonstrates the cluster age of different schemes. The cluster age is measured as the amount of time a cluster is active at each instant of time. The strength of a stable clustering algorithm should have comparatively longer cluster age. As shown in Fig 7 the cluster age decreases with the increase in the node velocity. This may be due to the link failure in the MANET. Compared to the other three schemes, HTMAC have longer cluster age even at higher rate of node mobility.

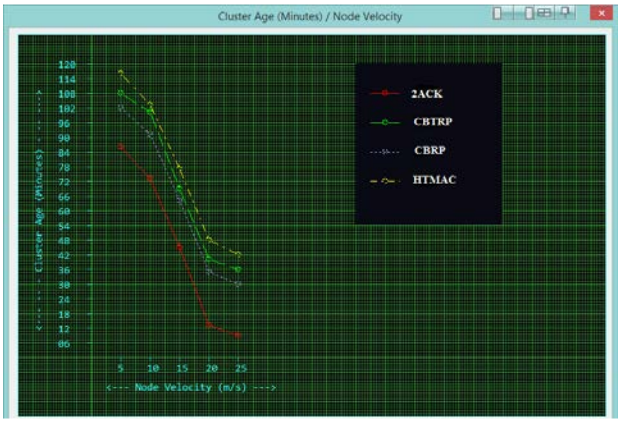


Figure 7: Cluster age with node velocity

6.3 Efficiency of HTMAC algorithm

The efficiency of proposed algorithm is measured in terms of performance parameters such as cluster overhead, message rate and security as shown Fig 8, Fig 9 and Fig 10.

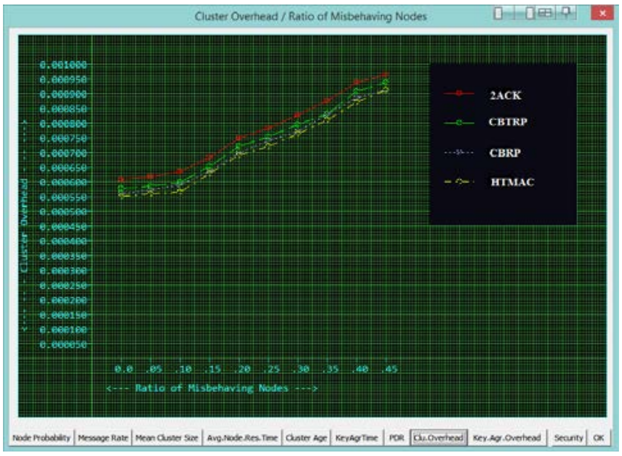


Figure 8: Cluster overhead with misbehaving nodes

The cluster overhead includes the cluster organization and maintenance in the ad hoc network. The efficiency of any clustering algorithm depends on its ability to provide stable clusters. Our proposed scheme shows a minimum overhead percentage when the ratio of misbehaving nodes are minimum as shown in Fig 8. Whereas, the overhead increases to 0.08% for maximum ratio of misbehaving node, which is very much low compared to the existing schemes.

One of the important parameter that determines the efficiency of a clustering scheme is the control message rate with respect to the node velocity. It measures number of updates within a cluster by each node per second whenever a node join or leave the cluster. With Fig 9, we can compare the variations in the message rate for different schemes. Initially the message rate increases with the change in topology. It is clearly shown in Fig 9 that the HTMAC scheme's mobility adaptiveness lowers the message rate with cluster size reduction as the node velocity increases beyond 20m/s.

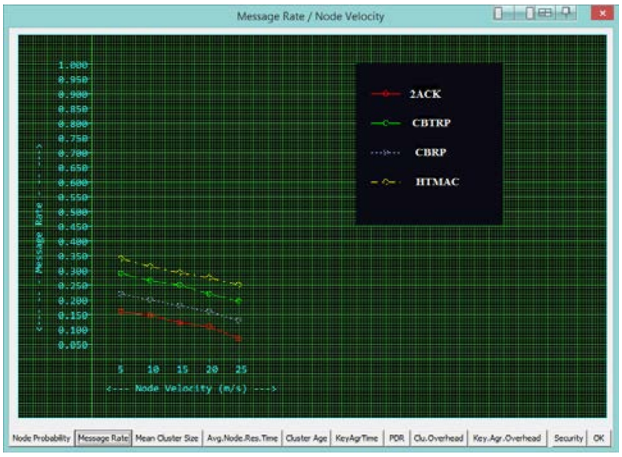


Figure 9: Control message rate

The Fig 10 shows the rate of security, which is considered as another significant parameter that measures the clustering algorithm's efficiency. The hackman tool along with the qualnet simulator verifies different attackers at regular time interval. The HTMAC scheme shows a higher rate of security to different attacks compared to other three schemes. A maximum of 97% security is achieved for minimum node mobility. The security level drops slightly to 93% when the node velocity reaches the maximum of 25m/s.

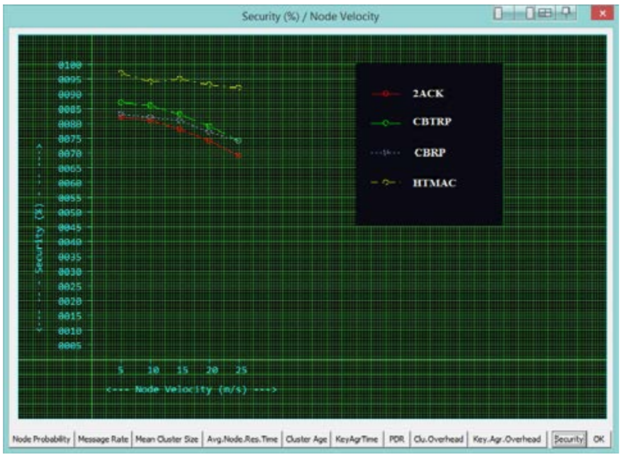


Figure 10: Security rate

7 Conclusion

In this paper we have address a distributed hexagonal trust based mobility aware clustering scheme (HTMAC) for mobile ad-hoc networks. Unlike the existing techniques, we have proposed HTMAC to efficiently partition the network into non-overlapping clusters of trustable nodes. Our approach enables each node to establish trustability with other interacting nodes, in each hexagonal cluster, with minimal complexities in header selection and maintenance. Simulation results shows that our scheme achieves *beneficial over (a) mobility adaptiveness (b) cluster stability with reduced overhead of clustering and cluster maintenance (c) control message rate and security.* Therefore, our scheme, HTMAC, can be adequately adopted for infrastructural less and dynamic wireless ad-hoc networks.

Acknowledgment

This research is supported by All India Council for Technical Education (AICTE), Government of India.

References

[1] Ratish Agarwal and Dr. Mahesh Motwani, “Survey of clustering algorithms for MANET”, International Journal on Computer Science and Engineering Vol.1, issue: 2, 2009, pp. 98-104.

[2] Abdelhak Bentaleb, Abdelhak Boubetra, Saad Harous, “Survey of Clustering Schemes in Mobile Ad hoc Networks”, Communications and Network, 2013, pp 8- 14.

[3] J.Y. Yu, P.H.J. Chong, A survey of clustering schemes for mobile ad hoc networks, IEEE Communications Surveys and Tutorials 7 (2005), http://dx.doi.org/10.1109/COMST.2005.1423333.

[4] M. Ni, Z. Zhong and D. Zhao. “MPBC: A Mobility Prediction-Based Clustering Scheme for Ad Hoc Networks,” IEEE TVT, Vol. 60, No. 9, 2011.

[5] P. Basu, N. Khan, and T. D. C. Little, “A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks,” in Proc. IEEE ICDCSW’ 01, Apr. 2001, pp. 413–18.

[6] Y. Zhuang, T. A. Gulliver, and Y. Coady, “On Planar Tessellations and Interference Estimation in Wireless Ad-Hoc Networks”, IEEE Wireless Communication Letters, Vol.2, No. 3, 2013.

[7] J.H. Cho, K.S. Chan, I.R. Chen, “Composite trust-based public key management in mobile ad hoc networks”, ACM 28th Symposium on Applied Computing, Coimbra, Portugal, 2013.

[8] R. Ferdous, V. Muthukkumarasamy, and E. Sithirasenan, “Trust-based cluster head selection algorithm for mobile ad hoc networks”, Proc.Int. Joint Conf. IEEE TrustCom, 2011.

[9] Z.Wei, H.Tang, F. Richard Yu, M. Wang, and P. Mason, “Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning”, IEEE Transaction on Vehicular Technology, Vol. 63, No. 9, 2014.

[10] K. Liu, N. Abu-Ghazaleh, K. Kang, “Location verification and trust management for resilient geographic routing", 2007.

[11] J.-H. Cho and I.-R. C. Kevin Chan, “A composite trust-based public key management in mobile ad-hoc networks,” ACM 28th Symposium on Applied Computing, Trust, Reputation, Evidence and other Collaboration Know-how (TRECK), March 2013.

[12] Fan.P, Li.G, Kai Cai, and Letaief.K.B, “On the Geometrical Characteristic of Wireless Ad-Hoc Networks and its Application in Network Performance Analysis”, IEEE Transaction on Wireless Communications, Vol. 6, No. 4, 2007, pp 1256 - 1265.

[13] Kao.B, Lee. S.D, Lee.F, Cheung.D, and Ho.W.S, “Clustering Uncertain Data Using Voronoi Diagrams and R-Tree Index”, IEEE Trans. Knowledge and Data Eng, vol. 22, no. 9,2010, pp 1219 - 1233.

[14] Stojmenovic.I, Ruhil.A.P and Lobiyal.D.K, “Voronoi diagram and convex hull based geocasting and routing in wireless networks”, Wireless. Communications and Mobile Computing,vol 6,2006, pp 247-258.

[15] Zhuang.Y, Gulliver. T. A, and Coady.Y, “On Planar Tessellations and Interference Estimation in Wireless Ad-Hoc Networks”, IEEE Wireless Communication Letters, Vol.2, No. 3, 2013, pp 331 - 334.

[16] Jingwei.H and David.N, “A calculus of trust and its application to pki and identity management”, In Proc. 8th Symposium on

Identity and Trust on the Internet, 2009, pp 23-37.

[17] Jiang, M., Li, J., & Tay, Y. C, “Cluster based routing protocol (cbrp)’, Internet Draft, MANET working group, 1999.

[18] Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K., “An acknowledgment-based approach for the detection of routing misbehavior in MANETs’, IEEE Transactions on Mobile Computing, 2007, pp 536–550.

[19] H. Safa, H. Artail, and D. Tabet, “A cluster-based trust-aware routing protocol for mobile ad hoc networks,” Wireless Networks, vol. 16, no. 4, 2010, pp. 969–984.