Topology Management based Energy balancing Model for IPS in MANET using MEC Clustering Algorithm

T. Parameswaran
Assistant Professor
Department of computer science and Engineering
Anna University of Technology, Coimbatore, India

C. Palanisamy, PhD
Professor and Head
Department of Information Technology
Bannari Amman Institute of Technology, Sathy, India

K. Madheswari
PG Scholar
Department of computer science and Engineering
Anna University of Technology, Coimbatore, India

ABSTRACT

In Mobile Ad-hoc Networks, the topology management is a crucial factor that plays a vital role to maintain the node cooperation and stability of the network in unpredicted movements of the nodes. Moreover, the resource consumption imposes problem with mobile nodes due to the variations of resource availability. The Intrusion Prevention System (IPS) offers more supportability for wired and wireless networks than ad-hoc networks besides, the IPS provides support for more trusted with low mobility ad-hoc networks. Nodes energy level is private information, so the nodes may behave selfishly and may not provide truthful information about it resource availability and avoids being a cluster head. The stability of the network topology may depend on smooth affiliations and re-affiliations of new node entering into the cluster. The clusterhead election process consumes more energy compared to energy required for data transfer. In this paper we propose MEC (Mobility, Energy and Credit) Clustering Algorithm in order to balance resource consumption among all nodes and enhance the network stability. The node with low mobility, trustiness and more remaining energy is elected as cluster head. Elected leader is responsible for providing IPS for the entire cluster. Our proposed algorithm provides incentives in the form of credits to encourage the nodes to honestly participate in the leader election process and decrease the percentage of selfish nodes in the network.

General Terms

Topology, Intrusion Prevention Systems, Random based approach, Connectivity Model, Distributed clustering algorithm (DCA), Weight-Based Adaptive Clustering Algorithm (WBACA), Connectivity, Energy and Mobility driven weighted Clustering Algorithm (CEMCA).

Keywords

Cost of analysis, credit system, incentives, mobility, staying time, remaining energy, and MEC algorithm.

1. INTRODUCTION

The Firewall allows all the outgoing data strings watching all the incoming data flow and guards the network from unwanted taken for granted activities, disturbances and attacks like an armor. It also monitors and scrutinizes all the information passing through, in and out of Mobile Ad Hoc Networks. If the Firewall encounters any fraudulent practices, they are just stopped from entering the network. A Firewall simply finds out and stops the unauthorized access. The Intrusion Prevention system (IPS) [9] is employed for the purpose of identifying a fraudulent activity to block any attempt to kill the network itself and finally to report such a coup attempt.

In an Ad-hoc network, there is no fixed infrastructure. For instance, there are no base stations, proxy or firewall settings where IPS (Intrusion Prevention systems) can be deployed. So each mobile node may need to run on its own Intrusion Prevention Systems in order to prevent malicious activity. This is ineffective in terms of resource utilization since mobile nodes are energy restricted.

There are several problems associated with wireless networks in general and MANETS in particularly (a) Energy constraints and; (b) dynamic topology configuration. The first one arises from the nature of the nodes formation in Mobile ad-hoc Networks, since the limited power resources of supply batteries [11]. As for the dynamic topology problem, it derives from the unpredicted mobility of the nodes and causes extra problems in the network's stability. Consequently, these two problems affect network lifetime and delivery processes within MANETs. In this article, we proposed a novel clustering algorithms for reliable network stability and trusted IPS services.

The common approach is to divide the MANET into set of one-hop clusters where each node belongs to at least one cluster. The nodes in each cluster elect a cluster head which provides intrusion prevention systems for non cluster head nodes. Lot of issues associated with electing unsurpassed node as cluster head. The problems are :(1) unfortunately, the nodes energy level is a private information, not disclosed publically, and thus not verifiable. Since nodes may behave selfishly, they may not provide truthful information about their resource level to avoid being the leader if there is no mechanism to motivate them. (2)Once the node is elected as a cluster head it behaves maliciously and may not provide IPS service for elected nodes. The malicious nodes try to deceive other nodes in order to save its energy and give a path for adversarial networks. The node with malicious behavior should be punished and removed from the network. (3) Due to the dynamic nature of the mobile nodes, their affiliations and re-affiliations to and from clusters may disturb the stability of the network and increases the number of election process. Election process consumes more energy compared to energy required for data transfer. Moreover, the stability of the cluster would be significantly affected. By electing low mobility node as cluster head, may decrease frequent election process as well as increase the cluster stability. Specially, we propose new clustering algorithm for cluster heads, that would be significantly overcome the above mentioned issues by consider the nodes' mobility, energy level, credit (incentives for serving others).

2. RELATED WORK

Several cluster head election algorithms [5] have been proposed for mobile ad-hoc networks (MANET) that assume link stability, mobility, connectivity, weight and energy and are therefore closely related to our work.

Distributed Clustering Algorithm (DCA): This approach [8] allows the choice of cluster head based on greater weight associated with it. Weight of the node is inversely proportional to its speed (Weight α (1/Speed)); the low mobility nodes are elected as cluster heads. Since these nodes do not move or move slower than other nodes, this will increase longer life of the cluster. Problems associated with DCA are: (1) the main assumption is that during the clustering process mobile nodes are stable, need not to move. This is not possible due to the dynamic nature of mobile nodes. (2)Energy level of the node is not taking into account during the clustering process; hence leader may die faster compared to all other nodes and leads to unbalanced resource consumption. (3) There is no mechanism to control selfish and malicious behavior of the node while providing IPS service for the elected nodes.

Weight-Based Adaptive Clustering Algorithm (WBACA): The clustering approach [4] presented in WBACA is based on the availability of position information via a global positioning system (GPS). The WBACA considers following parameters of a node for cluster head selection: Transmission power, transmission rate, mobility, battery power and degree of connectivity. Each node is assigned a weight that indicates its suitability for being cluster head. The node with the smallest weight is chosen as the cluster head. Problems associated with WBACA are: (1) when topology of cluster is changed or link with cluster head is disconnected due to mobility of cluster member nodes, it performs re-clustering, thereby lowering stability of cluster. (2) There is no control mechanism for selfish and malicious node.

Connectivity, Energy and Mobility driven weighted Clustering Algorithm (CEMCA): The CEMCA [6] considers following parameters of a node for cluster head selection: lowest node mobility, highest node degree, and highest energy level, best transmission range. Normalized value of mobility, degree and energy level is calculated and is used to find the weight for each node. The node broadcast its weight to their neighbors in order to choose the best among them. After this, a node that has the best weight is chosen as a cluster head. This algorithm is completely distributed and all nodes have the equal chance to be a cluster head. But there is no control mechanism to control selfish and malicious behavior.

Random Based Approach: Unfortunately, with the random model [1], each node is equally likely to be elected without considering its remaining resources. With this election scheme, some nodes will die faster than others, leading to a loss in connectivity and potentially breaks the network. There is no control mechanism for selfish and malicious nodes.

Connectivity based approach: The connectivity index-based approach [2] elects a node with a high degree of connectivity even though the node left with little resources. In this approach the same node is always elected as cluster head which leads to die faster than other nodes. There is no incentive for cluster head for serving other nodes.

All the above methods are introduced in order to balance the resource consumption among the nodes. Unfortunately, the above solutions did not consider the potential selfish behavior of nodes. Nodes may misbehave since they are not willing to spend their resources for serving others. At the same time, they benefit from others' services.

Mobile Ad hoc networks are subject to various kinds of attacks such as masquerading, man-in-the-middle, and replaying of messages. Deploying security mechanisms is difficult due to natural of Mobile Ad-hoc networks, such as the high dynamics of their topology (due to mobility and joining/leaving cluster), limited resources of each mobile node.

The design of security service in ad hoc networks is not to depend on any centralized entities, because such entities would obviously be easy to attack, and their reachability could not be guaranteed at all times for all participants of the network[12]. Therefore, it is not possible to implement a centralized, trusted entity to verify an authorized node. Each node in the network must protect themselves from Un-authorized nodes.

Cluster based MANETs focused on how to select reliable and trustworthy cluster head to provide IPS services, but they ignored the cluster head security after its election. During the life time of the Mobile Ad-hoc Networks, packets delivery phase takes much more time than the cluster election phase. That means cluster nodes are more likely to be compromised after the election process even if they were trustworthy in the past [10]. Therefore trust management of detecting and rejecting malicious attacks from betrayed malicious cluster heads is very critical. In this paper, we developed new credit model to solve this problem.

3. MEC ALGORITHM

3.1 Problem statement

Selfish nodes do not provide IPS service to other nodes while at the same time benefiting from others' services. From our experiments, selfishness reduces the efficiency of an IPS since fewer packets only inspected over time. Here, we modeling a MEC, clustering algorithm for electing a leader IPS that perform prevention process from malicious activity.

Our solution is focused to balance the resource consumption among all the node and increase the overall life time of an MANET. In this model incentives are provided in the form of credits to encourage the nodes to honestly disclose their resource level and truly participate in the cluster head election process. The credit is used to monitor the cooperative behavior of nodes where misbehaving nodes are punished by preserving the IPS service. Credits are calculated based on the mechanism known as [3] Vickrey, Clarke and Grove (VCG) which is mainly focused on truth-telling strategy. Moreover, once a member node is associated with a cluster head, it does not re-associate to a new head until it goes out of the transmission range of its current cluster or the head drains out of battery power. This reduces the number of re-affiliations and reduces the cluster maintenance cost. This is effectively achieved by MEC algorithm.

3.2 Topology Management

Several factors will affect the overall performance of any clusterhead election algorithm in an ad hoc network. For example, node mobility may cause link failures, which will negatively impact IPS services [13] [14]. Network size, control overhead, and traffic intensity will have a considerable impact on network scalability. These factors along with inherent characteristics of ad hoc networks may result in unpredictable variations in the overall network performance. To meet the requirements imposed by our MEC algorithm, topology construction is based on the following Assumptions:

1. Each node belongs to at least one cluster.
2. Network is divided into set of 1-hop neighbors.
3. No two cluster heads can be neighbors.
4. Number of nodes in a cluster is limited to seven. If the cluster size exceeds seven, then excess nodes become member of new cluster.
5. To make secure communication among the nodes, nodes information can be classified into three parts
   (a) Protected: Location information have to be accessible for authorized neighbors. It should not be disclosed to unauthorized neighbors.
   (b) Public: Number of neighbors, velocity of the node can be disclosed to all the nodes in the network.
   (c) Private: Energy level is private information. It should not be disclosed to any node.

To make our clusterhead election algorithm scalable, to avoid long-range traffic, and to facilitate the optimal reachability of clusterhead to other nodes, we are limiting the cluster size to seven.

3.3 Analysis of cost function

The objective of selfish node is to maximize its utility (payoffs). Therefore, incentives must be given to nodes to honestly participate in the election process. Incentives are modeled in terms of credit of node. Credit is used to decide whom to trust and motivate nodes to truthfully disclose their private information about their cost. The cost function aggregates the following metrics: Low Mobility, high energy and more credited node (trusted node). The node which is having the smallest cost of analysis function is elected as cluster head.

In our model, the default value of the credit at the initial cluster step-up time is fixed value (CR_0=1).A misbehaving node is punished by reducing its credits (TH<0) and stop clustering services when the credit reaches less than the predefined threshold (TH=0).

3.4 Calculation of node mobility

Due to dynamic nature of MANET the mobility of nodes cannot be ignored. Therefore, Nodes Mobility [7] plays a vital role in cluster maintenance. The node with low mobility, thus we choose to be the one of the key factor to elect a cluster head in order to enhance stability of the cluster.

Principally, we consider the mobility of node by calculating the average of the distances covered by it in last n time slots.

Total distance moved at time t is D_t

$$\mathrm{D_t} = \sum_{\mathrm{i=t-n}}^{\mathrm{i=t}} \mathrm{Dist\ i} \qquad (1)$$

Where i=t is current time.

Thus, mobility M=Total distance $D_{t\,/}$ n

3.5 Calculation of Residual Energy

Ad-hoc mode of operation does not have any fixed infrastructure. So nodes communicate directly with all other nodes which are in its transmission range because of absence of base station. Since the nodes are ready to receive traffic from their neighbors and does not enter into sleep state [7]. However, a node can enter into idle state when it is continuously listens to the network and consumes energy which is almost same as energy consumption in receiving traffic.

For easy understanding, we have taken a linear model for the energy consumption cost of mobile nodes for sending and receiving a packet. So the energy required for ordinary node is calculated as follows.

$$\text{Energy}_{\text{ordinary}} = \text{m}_{\text{send / receive}} \times \text{size packet} + \text{c}_{\text{broadcast}} \qquad (2)$$

Where m is incremental cost and c is a fixed cost that represents a broadcast communication.

This calculation differs for the cluster head. The energy consumption of a cluster head basically depends on the following metrics:

1. The traffic forwarded by the cluster head
2. No. of members served by the cluster head
3. Total transmission power utilized by the cluster head in serving the members.

Energy consumed by the cluster head is calculated as

$$\mathrm{Energy_{head}} = \alpha * |\mathrm{n_i}| + \beta * \mathrm{Traffic_{bcast}} + \gamma * \sum_{\mathrm{v}\,\epsilon\mathrm{i}} \mathrm{dist(v, v)} \qquad (3)$$

Where $|n_i|$ represents a cardinality of cluster,$Traffic_{bcast}$ Represents the cost of energy consumption in traffic forwarding, $\sum_{v\,\epsilon i} dist(v,v)$ is the total transmission power.

α, β, and γ are weighting parameters (α+ β+ γ=1). The values of these parameters are kept supple so that they can be changed as per network changes. In case, the network traffic is very high β can be given more weight age than others. For dense network the cardinality of cluster are more, the weight age of α dominates the other two parameters.

3.6 Cost of analysis function

The cost of analysis function is calculated based on credit value, remaining energy and mobility of node. The credit of node is denotedCR_i. Every node has sampling budget based on its credit. The percentage of sampling is defined as

$$\mathrm{PS_i} = \frac{\mathrm{CR_i}}{\sum_{\mathrm{i=1}}^{\mathrm{N}} \mathrm{CR_i}} \qquad (4)$$

The elected leader provides IPS service for the elected members based on their sampling budget.

Cost of analysis function is formulated as follows:

$$\mathrm{C_i} = \begin{cases} \infty & \text{if } (\mathrm{E_i} < \mathrm{E_{IPS}}), \\ \dfrac{\dfrac{\mathrm{CR_i}}{\sum_{i=1}^{N} \mathrm{CR_i}} \times \mathrm{M_i}}{\mathrm{E_i}} & , \quad \text{otherwise} \end{cases} \tag{5}$$

Where,
C_i = The cost of analysis function for a single packet,
E_{IPS} =The energy needed to run IPS for at least one time slot,
$CR_i =$ Credits (payment) for the node,
M_i=Mobility of the node,
E_i=Energy level of the node

The nodes have an infinite cost of analysis if its residual energy is lesser than the energy required running the Intrusion Prevention Systems for at least one time slot. The cost of analysis function is directly proportional to credit of the node and mobility, but inversely proportional to the Energy level. On the other hand, if energy of the node is high and mobility is low, then the cost of analysis function becomes smaller. Our aim is to elect the most efficient node as leader that will have smallest cost-of-analysis function.

3.7 Credit system model

Before the calculation of payment, it is necessary to show how the payment in the form of credit can be used to:
1) Encourage selfish nodes to reveal truthful information about their resource level.
2) Malicious nodes can be punished by excluding from the network.
3) Moreover, credit can be used to decide whom to trust.

To encourage the nodes behave normally in every election process, the cluster service is related to the nodes' credit. This will create a competitive setting that motivates the nodes to behave normally by enlightening honest information. The initial value of credit is set to one (CR=1) and threshold value is set to zero (TH=0) .For each and every election round the credit is compared with threshold. If credit is greater than the predefined threshold, then credit value summed with previous credit value.

The node with high credits can enjoy the benefits of clustering services. In case the nodes credit value is lesser than predefined threshold, punishment system is called which detects the credit value from already available credits.

Pseudo code for Credit system Model

```
Begin monitoring mechanism
Evaluate credit for each node
Initial credit=1
Predefined threshold=0
If (credit > predefined threshold)
Credit = previous value + current value
Update credit
Call IPS service system
If node behave malicious
Credit = previous value - current value
If (credit < 0)
Call punishment system (excluding from network)
End
```

3.8 MEC-payment design

MEC algorithm provides payment to the elected leaders for serving others (i.e. offering the prevention service). The payment is based on a per-packet price that depends on the number of votes the leader get. The nodes that do not get any vote from others will not receive any payments. The payment is in the form of credits, which is used to allocate the leader's sampling budget for each node. Hence, every node will strive to increase its credit in order to get more IPS services from its corresponding cluster head.

The Total payment is formulated as follows:

$$\mathrm{P_k} = \sum_{\mathrm{i \epsilon N}} \mathrm{v\,t_k(C,i)B\rho_k}, \tag{6}$$

Where P_k = Total payment received by the node,
$\mathrm{vt_k(C,i)}$ = 1 if a node i votes for a node k,
$\mathrm{vt_k(C,i)}$ = 0, otherwise
B = sampling budget and $\rho_k$is payment per-packet

Payment per packet is calculated as follows:

$$\mathrm{\rho_k} = \mathrm{C_k} + \frac{1}{\sum_{\mathrm{i \epsilon N}} \mathrm{v\,t_k(C,i)}} \times$$

$$\left[\sum_{\mathrm{j \epsilon N}} \mathrm{c_j} \sum_{\mathrm{i \epsilon N}} \mathrm{v\,t_j(C|c_k = \infty, i)} - \sum_{\mathrm{j \epsilon N}} \mathrm{c_j} \sum_{\mathrm{i \epsilon N}} \mathrm{v\,t_j(C,i)}\right] \tag{7}$$

Table1. A Leader IPS Example

Nodes	Credit Round-5	Cost-of-analysis	Credit Round-6
N_1	110	10	110
N_2	90	6	90
N_3	60	8	60
N_4	160	4	160
N_5	130	7	170
N_6	10	3	110
N_7	80	12	80
N_8	100	4	195
N_9	140	5	140
N_{10}	120	9	165

Example 1: we consider a cluster of 10 nodes with 30% of selfish nodes (3 nodes) shown in figure.1.MEC algorithm is repeatable; we present the election process at 6th round. We assume that the credit at the 5th round is given in the first row of table1. According to node type (selfish/normal), nodes declare the cost of analysis using the equation (5), node N_6 has the lowest cost of analysis function. Equation (7) is used to compute the expense of node 6, which is in the form of credit. In case the node 6's cost is ∞, after that the node N_1 would be voted for nodes N_3 and N $_2$, and nodes N_4 and N_6voted for N_4.

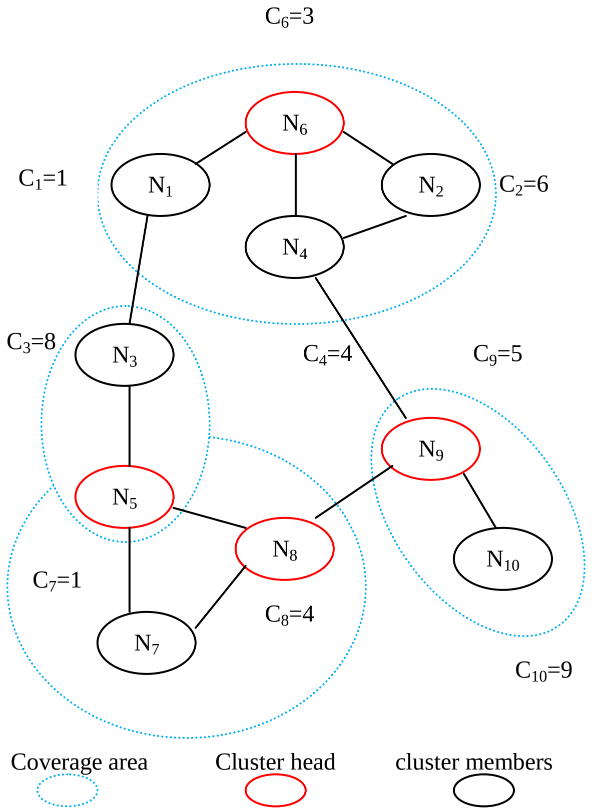


Figure.1. An example of leader election

Payment per-packet

$$\rho_6 = 3(\text{real cost}) + \frac{1}{4(\text{voted nodes})} \times$$

$$[8 \times 1(\text{N3 cost}) + 4 \times 3(\text{N4 cost}) - 3 \times 4(\text{N6 cost})]$$

$$\rho_6 = 3(\text{real}) + 2(\text{incentive}) = 5(\text{payment})$$

Incentive =5-3=2 units per-packet

Since the node utility is 2, which represents incentive gained by the node. On the other hand, the cluster is providing IPS service with the payment of 3 units of credits at the same time as receiving the payment of 5 units; this incentive will be used for augment its prevention service in future. Here we are motivating the nodes to honestly participate in the leader election process and provide truthful information regarding the resource availability.

Distribution of sampling budget

$$\text{PS}_\text{i} = \frac{\text{CR}_\text{i}}{\sum_{\text{i}=1}^{\text{N}} \text{CR}_\text{i}}$$

$$\text{S}_1 = \frac{110 \times 20}{470} \quad (110 + 90 + 160 + 110 = 470)$$

$$\text{S}_2 = \frac{90 \times 20}{470} = 4 \text{ (instead of 5 packets)}$$

$$\text{S}_4 = \frac{160 \times 20}{470} = 7 \text{ (instead of 5 packets)}$$

$$\text{S}_6 = \frac{110 \times 20}{470} = 5 \text{ (instead of 5 packets)}$$

Here node 4 is having more credit value so that it can use more clustering services (7 packets instead of 5) such as intrusion prevention system, routing priority, packet forwarding. Purely, in our mechanism intrusion prevention service is provided according to its credit value (trust worthy). From this we can create a competitive environment among the nodes that motivate selfish nodes to behave normally.

Presence of selfish nodes: selfish nodes may over estimate or under estimate its cost. Unfortunately, selfish nodes are not able to enjoy the benefit of forged value due to the limitations of our MEC clustering algorithm. The node 6 may be over estimate its value (forged value); Assume that cost of analysis is 5 instead of 3 units. This would not at all make a node better-off in two cases: 1) if the node N_6 really has a cost function, then our mechanism may avoid the node from being elected, it will lose the payment. 2) Then again, if node N_6 stills wins, then its payment leftovers same since the payment does not depend on the price it reports. The node N_6 may under declare a forged value; assume cost of analysis function is 1 instead of 3. But the node receives the true payment 5 units and there is no use of under declaration .Strictly, our mechanism will give payment based on node’s original value and not based on forged value.

Over declaration

payment per – packet

$$\rho_6 = 5 + \frac{1}{4} \times [8 \times 1 + 4 \times 3 - 5 \times 4]$$

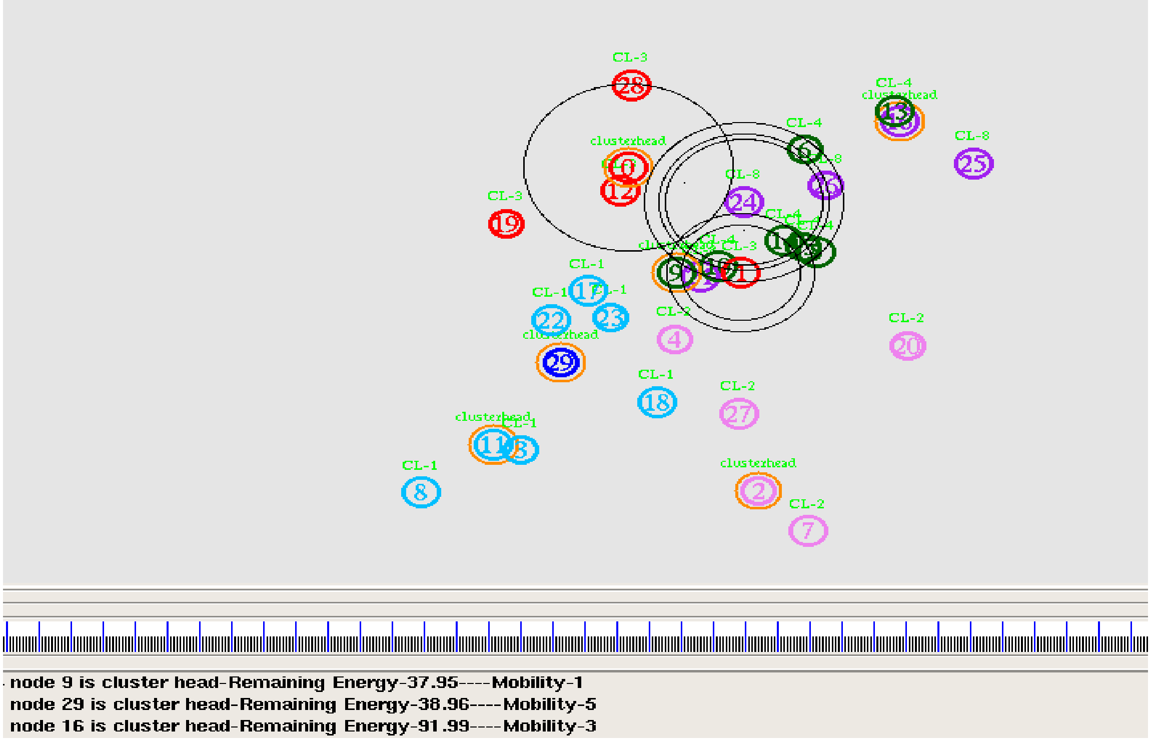
$$\rho_6 = 5 + \tfrac{1}{4} \times [0] = 5 \text{ (no incentive)}$$

Under declaration

payment per – packet

$$\rho_6 = 1 + \frac{1}{4} \times [8 \times 1 + 4 \times 3 - 1 \times 4]$$

$$\rho_6 = 1 + \tfrac{1}{4} \times [16] = 5 \text{ (same payment)}$$



node 9 is cluster head-Remaining Energy-37.95----Mobility-1
node 29 is cluster head-Remaining Energy-38.96----Mobility-5
node 16 is cluster head-Remaining Energy-91.99----Mobility-3

Figure .2 Topology management based Clusterhead Election process

4. LEADER ELECTION PROCESS

Our MEC algorithm is proposed based on the following criteria: first, elect a more suitable node for providing Intrusion Prevention Systems on behalf of voted nodes. Second, nodes' remaining energy level is private information, cannot be disclosed. So the nodes do not provide real information. Third, Energy level alone is not sufficient factors to decide about cluster head. Once a node is elected as cluster head, it will stay in the cluster at least one time slot. Specifically, mobility take place another important role so that nodes with less mobility can be choose in turn to decrease number of affiliations and re-affiliations to and from the cluster which enhances the cluster stability.

We assume that every node maintain a table about their neighbors for routing purposes. To start an election, our algorithm uses for types of messages and five types of tables.

Messages

Initiate-Election: used by all the nodes to start the election process

Hello: used to announce cost of node

Vote: sent by every node to elect a cluster head

Acknowledge: sent by the leader to announce its payment and conformation of leadership.

List of Tables

Member-Table (k): The list of member nodes, those voted for the cluster head (k)

Credit-Table (k): The credit value of node k and maintain the record of credit of all other nodes.

Neighbors (k): set of k's neighbors

Cluster-Head (k): The ID's of node k's cluster head. If node k is running on its own IPS then the variable contains k.

Leader (k): It is set to TRUE if node k is leader.

5. SIMULATION RESULTS

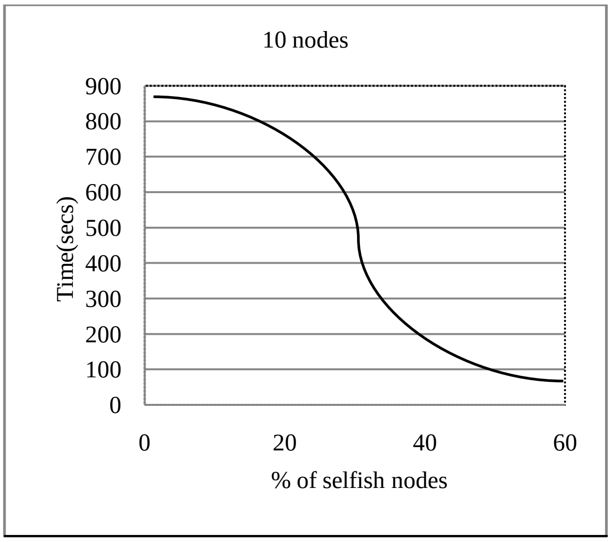


Figure .3 Impacts of selfish nodes on normal nodes

NS2 is used to simulate our MEC algorithm, random model, and distributed clustering Algorithm. We simulate our algorithm of 10 to 30 mobile nodes in the presence of 30% selfish nodes. Initially, we allocate 10 to 100 joules to each node. We assume that energy required running IPS for one time slot is 10 joules and set the coverage area of each node to 200 meters.

Figure.2 shows cluster head can have only a predefined number of members to facilitate the optimal reachability of clusterhead to other nodes. Cluster size is limited to seven. If number of cluster nodes exceeds seven, then the excess nodes becomes the member of new cluster. Clusterheads are marked by orange color. The elected Clusterhead can have maximum remaining energy and low mobility than cluster members.

Figure.3 shows the impact of selfish nodes on the life of normal nodes .The result show that when there is a presence of more selfish nodes, normal nodes will carry out more duty and die faster.

In Figure.4 our model is compared with other two models to show the percentage of affiliations and re-affiliations. Our model significantly, reduces the number of associations and disassociations to and from the cluster, which potentially saves energy. Election process consumes more energy compared to energy required for data transfer.

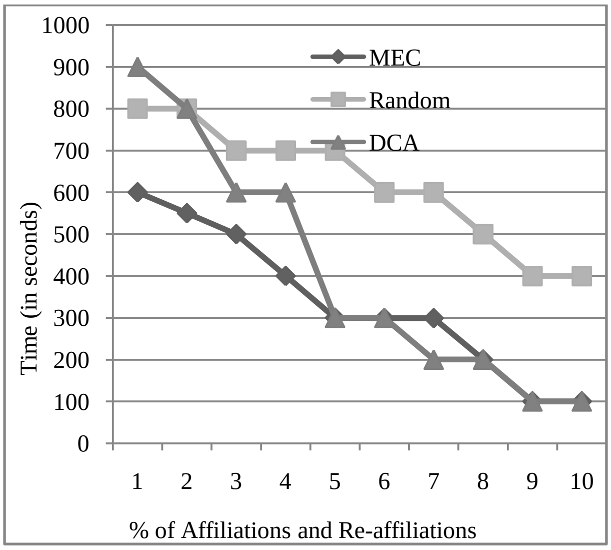


Figure .4.Stability of the cluster

Figure.5 shows that our model is able to balance resource consumption among all the nodes in the presence of selfish nodes.

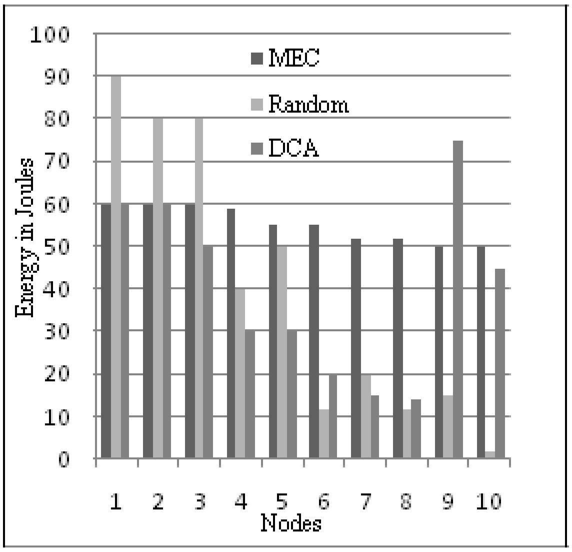


Figure.5 Balanced energy level -our MEC algorithm

6. CONCLUSION

Our proposed algorithm balances the highly variable amount of resource consumption among the nodes, and life time of an MANET is increased. Due to the credit model percentage of selfish behavior is significantly reduced. Moreover, our model is able to decrease the percentage of affiliations and re-affiliations to and from the cluster and enhances the network stability. Our model is also suitable for wireless sensor networks, military applications, routing services and centralized key distribution in MANET where, the nodes are energy limited

7. REFERENCES

[1] Y. Huang and W. Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks,” Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2003.

[2] O. Kachirski and R. Guha, “Efficient Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks,” Proc. IEEE Hawaii Int’l Conf. System Sciences (HICSS), 2003.

[3] A. Mas-Colell, M. Whinston, and J. Green, Microeconomic Theory. Oxford Univ. Press, 1995.

[4] S.K. Dhurandher and G.V. Singh” Weight-based adaptive clustering in wireless ad hoc networks” IEEE 2005.

[5] Ratish Agarwal, Mahesh Motwani “Survey of clustering algorithms for MANET “International Journal on Computer Science and Engineering Vol.1(2), 2009, 98-104.

[6] F.D.Tolba, D. Magoni and P. Lorenz “Connectivity, energy & mobility driven weighted clustering algorithm” in proceedings of IEEE GLOBECOM 2007.

[7] Suchismita Chinara, Santanu Kumar Rath “Energy Efficient Mobility Adaptive Distributed Clustering Algorithm for Mobile Ad Hoc Network” IEEE 2008.

[8] J. Y. YU and P. H. J. CHONG,”A Survey of Clustering Schemes for Mobile Ad hoc Networks, ”IEEE Communications Surveys and Tutorials, First Quarter 2005, Vol. 7, No. 1, pp. 32-48.

[9] Usman Asghar Sandh, Sajjad Haider, Salman Naseer, Obaid Ullah Ateeb “A Survey of Intrusion Detection & Prevention Techniques” IPCSIT vol.16 (2011) © (2011) IACSIT Press, Singapore.

[10] Wen Shen, Guangjie Han, Mengali cheng, Chuanzhu, Gang Hu, “Energy Prediction based Trust Manangement in Hierarchical Sensor Networks” IEEE 2010, Vol12-453.

[11] Christos I. Katsigiannis , Dimitrios A. Kateros, Eleftherios A. Koutsoloukas, NikoLaos D. Tselikas, and Iakovos S. Venieris “Architecture for reliable service discovery And delivery in MANETs based on power Management employing SLP extensions” IEEE Wireless Communications, October 2006.

[12] M. Bechler, H.-J.Hof, D. Kraft F. Pahlke, L.Wolf “A Cluster-Based Security Architecture for Ad Hoc Networks” IEEE INFOCOM 2004.

[13] Dmitri D. Perkins, Herman D. Hughes, and Charles B. Owen “Factors Affecting the Performance of Ad Hoc Networks” IEEE 2002.

[14] Chien-Chung Shen, Chavalit Srisathapornphat, Rui Liu, Zhuochuan Huang, Chaiporn Jaikaeo, and Errol L. Lloyd “CLTC: A Cluster-Based Topology Control for Ad Hoc Networks” IEEE transactions on mobile computing, vol. 3, no. 1, January-March 2004.