# COOPERATIVE CLUSTERING BASED SECURE LEADER ELECTION MODEL FOR INTRUSION DETECTION IN MANET

**R. Jasmin Reeda***

**A. Ananthakumari***

**Abstract:**

In this paper, we learn the leader election in the occurrence of selfish nodes for intrusion detection in mobile ad hoc networks. Leader election is the key to cluster strength and network performance. We propose a partner clustering algorithm (PCA) to elect right leader node for each cluster and divider the network into non overlapped 1-hop clusters. Specifically, our PCA adopts Coverage distance, transmission power as metrics to periodically choose proper leader node. One of the main obstacle in achieving this target is a node might act selfishly by untruthful about its resources and avoiding being elected. We present a solution based on the vickrey, Clarke, and groves solution provides nodes with incentives in the type of reputations to promote nodes in truthfully participating in the election process.

Keywords: **PCA algorithm, Intrusion detection, VCG approach.**

* Department of Information Technology, PSN College of Engineering and Technology, Tirunelveli.

## I. INTRODUCTION

Mobile ad hoc network is created by a set of movable wireless nodes,it does not having the permanent network infrastructure. There are a number of important MANET applications as battleground operations, mobile conferencing, home and group of people networking. MANETs are much weaker to attacks due to the open medium, dynamically altering network topology. Cryptographic mechanisms provide protection against some types of attacks from outer nodes, it will not protect against malicious interior nodes. Therefore, intrusion detection mechanisms are necessary to discover the Byzantine nodes. Intrusion Detection Systems [1] may be classified based on the data collection mechanism, as well as the technique used to detect events. In IDS method, the leader selection is considered necessary for key allocation and routing in MANET.

The election process can be both random [2] or connectivity based [3]. Both approaches can be used to decrease the overall resource utilization of IDSs in the network and select a leader node. The connectivity key-based approach elects a node with high amount of connectivity even though the node may have small property missing. among both election schemes, some nodes will pass away faster than others, leading to a failure in connectivity and division of network. The Cluster dependent leader election (CDLE), Cluster independent leader election approach select a leader node based on their resource level. But it partitions the network in to overlapped clusters.

In this paper, first we prevent nodes from behaving selfishly; we design incentives in the form of reputation to support nodes to truthfully join in the election scheme, the design of incentives is based on a standard mechanism design model, namely, Vickrey, Clarke, and Groves (VCG). Then we propose partner clustering algorithm (PCA) to elect suitable Cluster Head and partition the network into non overlapped 1-hop clusters. This algorithm decreases the percentage of leaders, single-node clusters, and greatest cluster size, and increases average cluster size.

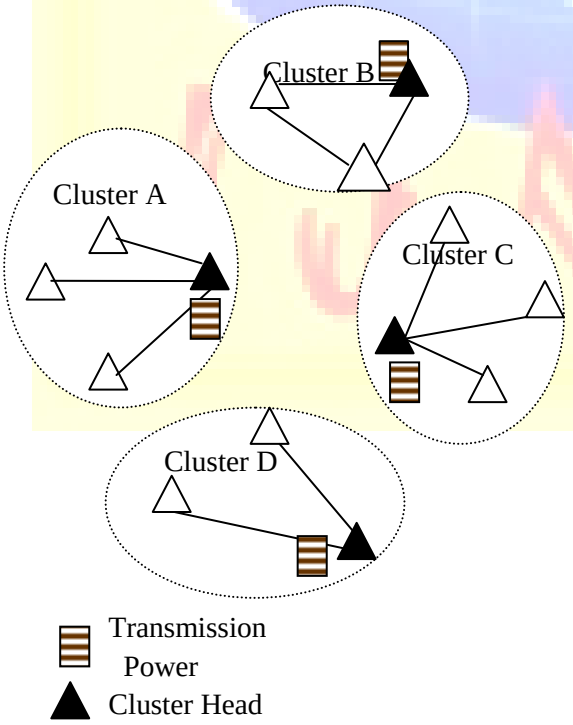

Fig1.Example development of leader Election in MANET.

## II. ANALYSIS OF MECHANISM DESIGN MODEL:

### A. Cost of Analysis function:

The cost of analysis function is a new significant component of the mechanism. The design of analysis function aims to achieve fairness among nodes in the logic that a node with less resources can have some probability to be elected as a leader. We divide nodes into l energy classes. Each node i is associated with an energy level, denoted by Ei, and a number of expected alive slots, denoted by nTi. Based on these requirements, each node i has a power factor PFi = Ei/nTi.

Every node has a sampling budget based on its reputation.The reputation of node i is denoted by Ri. The cost of analysis of each node can be calculated based on energy level, expected lifetime, and the PS of the node.

PS= $\frac{\text{Ri}}{\sum_{i=1}^{N} \text{Ri}}$ , Our Cost-of-Analysis Function is formulated as follows:

Cost-of-Analysis Function

/* Nodes execute this function to calculate their cost*/

1. if (Ei < Eids)
2. then
3. ci = ∞
4. Else
5. ci = $\frac{PSi}{PFi}$ = $\frac{\frac{\text{Ri}}{\sum_{i=1}^{N} \text{Ri}}}{Ei}$
6. End if

According to the above Cost of analysis function, if energy is less than the energy required to run the IDS, nodes have an infinite cost of analysis. This means its remaining energy is too low to run the IDS for an entire time-slot. Otherwise, the cost of analysis is calculated through dividing the percentage of sampling(PS) by the power factor(PF). The cost of analysis c is proportional to the percentage of sampling and is inversely proportional to the power factor. If nodes have sufficient PS, they are not ready to lose their energy for running the IDS. On the other hand, if the PF value is bigger than the cost of analysis becomes smaller since nodes have higher energy levels.

### B. Design of payment:

The payment design is based on a per packet price it depends on when the number of votes the elected nodes get. If the node does not catch the votes from others then the node will not get any payment. The payment is in the type of reputations, which are used to allot the leaders sample resources for each node. Hence any node will struggle to increase its reputation to receive more IDS services from its corresponding leader.

### C. Punishment Mechanism:

Our leader election mechanism is mainly used to encourage selfish nodes to behave normally in the leader's election process. However, a malicious node can disturb our election algorithm by claiming a fake low cost just to be elected as a leader. Once leader node was elected, the node does not provide Intrusion detection services, which ease the work of intruders. To catch and punish a misbehaving leader

who does not serve others after being elected, we have proposed in a decentralized catch-and-punish mechanism using random checker nodes to monitor the behavior of the leader.

## III. PARTNER CLUSTERING ALGORITHM:

In this sector we illustrate the cluster head suitability score calculation, leader node(cluster head) (CH) selection, Cluster creation and protection. Figure shows the three major steps of PCA.

Initial, the nodes estimate their appropriateness for being a Leader node. once the estimation, a suitability distribution mechanism is then exercised. As a final point, the nodes with higher suitability scores than their neighbors are selected as the leader node.

**Methodology Used:**

### A.CH suitability calculation:

CH suitability is calculated based on the Coverage distance, transmission power, and normal speed of all nodes in the network. Its suitability Score for being a CH according to the following formula:

$$\text{Score}= \frac{1}{Dn+Sn+Pt}$$

Where Dn is the coverage distance, Sn is the normal speed, Pt is the transmitted power; here a node with the largest Score is to be chosen as a CH.

### B. Suitability distribution:

Suitability distribution requires propagate the suitability information to all the nodes in the network. In every routing cycle, all nodes are update its cluster head suitability score and encapsulate it into a BEACON message. When the BEACON message is transmit, each neighbor receiving this BEACON and stores the score information. This stored score information is once more transmit with the next BEACON.

### C. Cluster construction and protection:

A node among the biggest score becomes a Cluster Head. Then, the elected CH adds its Cluster head information into its BEACON message and broadcasts it. The Cluster head neighbors receiving this message will join the cluster and become Cluster Members.

In suitability distribution, if the BEACONs message got lost due to collision or other issues, a node having a poorer suitability score may declare itself as a Cluster head. Therefore, two or more Cluster head in the similar 2-hop coverage area appear and compete for Cluster members. But, nodes will think that these CHs are for different clusters because they use the CH IDs to distinguish different clusters. i.e.) for every Cluster head it has its own cluster. Therefore, no clusters contain two or more Cluster heads.

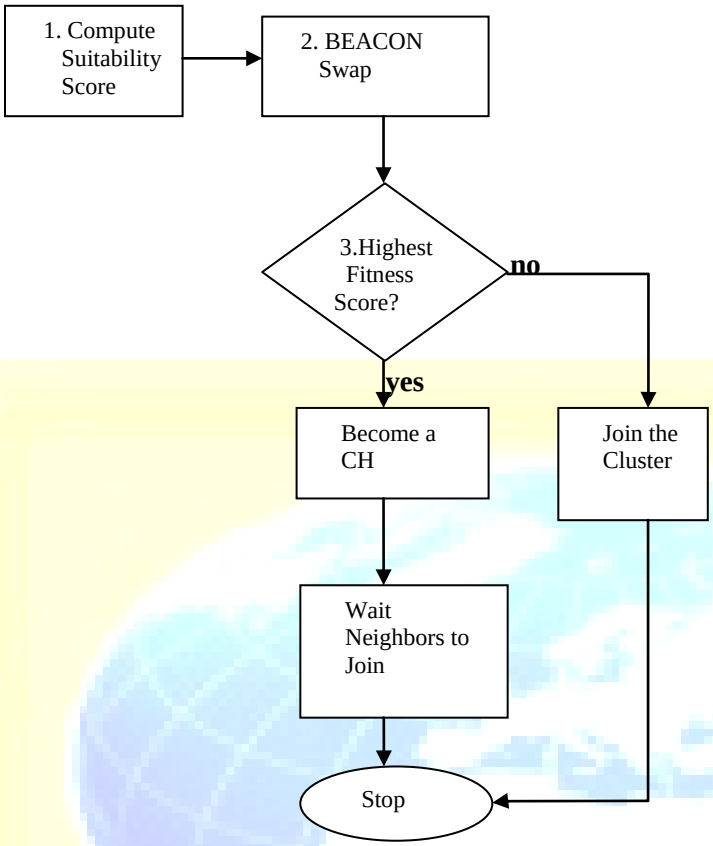


Fig2. PCA

## IV. EXPERIMENTAL RESULTS :

In this section Fig a**)** shows when the number of node increases,our algorithm is able to balance the energy consumption.fig b) indicates the number of leader nodes.The number of leaders for our model is high as compared to those of the existing systems that saves the energy of all nodes.

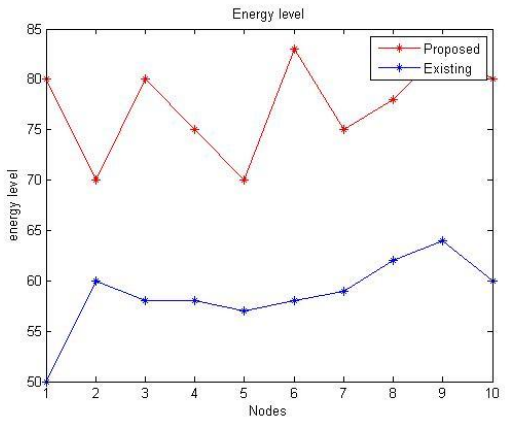


Fig) a. Energy level of our model.

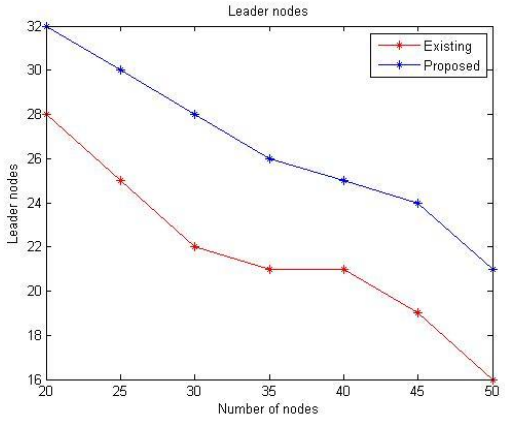


Fig b) Percentage of leader nodes

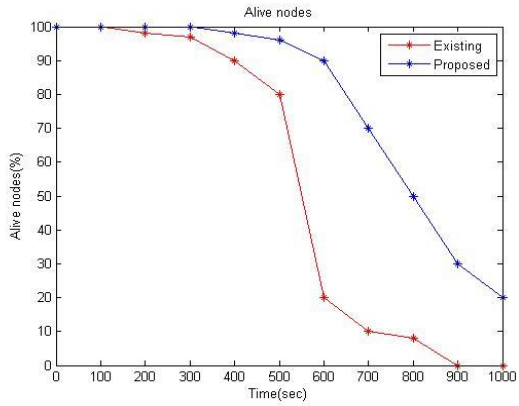


Fig c) Percentage of alive nodes

Fig c. shows the percentage of alive nodes.when the number of nodes increases the life time of nodes also increases i.e)increases the alive nodes.

From these experiments our algorithm is able to balance the energy consumption an also to reduce the cluster size and also avoid the overlapped clusters.

## V. CONCLUSION:

The unbalanced energy consumption of IDSs in MANET and the presence of selfish nodes have motivated us to propose an integrated solution for prolonging the lifetime of mobile nodes and for preventing the emergence of selfish nodes. The solution motivated nodes to truthfully elect the most cost-efficient nodes that handle the detection duty on behalf of others. To achieve this goal, incentives are given in the form of reputations to motivate nodes in revealing truthfully their costs of analysis. To implement our mechanism, we devised an election algorithm based on partner clustering algorithm PCA, to elect suitable CHs and partition the network into logically non-overlapped 1-hop clusters. Thus the way to reduce cluster size and optimal coverage we got an secure and energy efficient MANET.

## VI. REFERENCES


- Y.Xiao, X.Shen, and D.Z.Du, "A Survey on Intrusion Detection in Mobile Ad hoc Networks", pp. 170 – 196, 2006 Springer.
- 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.
- 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.
- A. Mas-Colell, M. Whinston, and J. Green, "Microeconomic Theory", Oxford Univ. Press, 1995.
- Suchismita Chinara and Santanu Kumar Rath**,** "TACA: A Topology Adaptive Clustering Algorithm for Mobile Ad hoc Networks", National Institute of Technology, Rourkela, Orissa, India.
- P. Krishna, N.H. Vaidya, M. Chatterjee, and D.K. Pradhan, "A Cluster-Based Approach for Routing in Dynamic Networks", Proc. ACM SIGCOMM Computer Comm. Rev., 1997.
- M. Bechler, H.J. Hof, D. Kraft, F. Pahlke, L. WolfA, "Cluster Based Security Architecture for Ad hoc Networks", Germany 2004 IEEE.
- Oleg Kachirski, Ratan Guha, "Effective Intrusion Detection Using Multiple Sensors In Wireless Ad hoc Networks", HICSS'03, 0-7695-1874-5/03 $17.00 © 2002 IEEE.
- Stefano Basagni, "Distributed Clustering for Ad hoc Networks", Australia June 2003.
- Vih-Chun Hu and Adrian Perrig, David B.Johnson, "Ariadne: Secure On Demand Routing Protocol for Ad Hoc N/w", Carnegie Mellon University, USA 2005 Springer.