# Secured Energy Efficient Mechanism for MANET

A.Suganya, Mr.G.Sivakumar, Dr.K.Ramasamy

**Abstract**— In Modern year a hasty development and extensive application of mobile ad hoc networks bear from security attacks and privacy issues which radically hamper their applications. To deal with the attacks, a huge selection of intrusion detection techniques such as authorization, authentication, key management schemes and cryptographic protocols have been developed. Clustering methods allow quick connection, topology management and enhanced routing of mobile ad hoc networks (MANET). This project introduces a new mechanism to divide the MANET into a set of clusters where each node belongs to not less than one cluster. The nodes in each cluster elect a leader node (cluster head) to serve for the whole cluster. To equilibrium the resource consumption weight based leader election model is used, which elects an optimal collection of leaders to minimize the overall resource consumption and obtaining secure communication using Diffie-Hellman key exchange protocol. In addition this paper also deals with LZW Compression to increase the lifetime of nodes by sending data quickly.

**Index Terms**— Clustering, Data Compression, Diffie-Hellman, Leader Election, LZW Compression, MANET, Security.

---

## 1 Introduction

MOBILE Ad hoc Networks have no fixed chokepoints /bottlenecks. This is very inefficient in terms of resource consumption since mobile nodes are energy-limited. The leader election process can be either random or based connectivity model (CM). Both approaches aim to reduce the overall resource consumption of the node in the network. However, we observe that nodes usually have dissimilar remaining resources at any certain time, which should be taken into account by an election scheme. In random model and connectivity index-based approach some nodes will expire faster than others, leading to a loss in connectivity and potentially the partition of network. Moreover, even when all nodes can truthfully reveal their resource levels, it remains a challenging issue to elect an optimal collection of leaders to balance the overall resource consumption without flooding the network.



## 2 Related Work

Haidar Safa et.al [5] have proposed A Dynamic Energy Efficient Clustering Algorithm for MANETs. The proposed algorithm elects first the nodes that have a higher energy and less mobility as cluster-heads, then periodically monitors the cluster-heads energy and locally alters the network topology or the clusters to increase the network lifetime by reducing the energy consumption of the suffering cluster-heads.

Tomas Johansson et.al [23] have proposed On Clustering in Ad Hoc Networks. It makes it possible to define a limit for the maximum size of the clusters as well as the maximum number of hops between a node and its clusterhead. The algorithm presented here has a time Complexity of O(d)2.

Sonia Buchegger et.al [29] have proposed Performance Analysis of CONFIDENT Protocol Cooperation of Nodes – Fairness In Dynamic Ad-hoc Networks. This protocol aims to detecting at detecting and isolating misbehaving nodes and recognizes the special requirements of MANET.

## 3 Existing Method

### 3.1 Leader Election Mechanism

Mechanism design is a sub-field of microeconomics and game theory. Mechanism design uses game theory tools to achieve the desired goals. The main difference between game theory and mechanism design is that the former can be used to study what could happen when independent players act selfishly. On the other hand, mechanism design allows a game designer to define

---


- *A.Suganya is currently pursuing masters degree program in computer and communication engineering in P.S.R.Rengasamy College of Engineering for Women, Sivakasi, India. E-mail: suganct@gmail.com.*
- *G.Sivakumar is currently working as Assistant Professor in Department of Electronics and Communication Engineering in P.S.R.Rengasamy College of Engineering for Women, Sivakasi,India, PH-7708304530. E-mail: gsivakvp@gmail.com.*
- *Dr.K.Ramasamy is currently working as Principal and Professor in P.S.R.Rengasamy College of Engineering for Women, Sivakasi, India. E-mail:ramasamy @psrr.edu.in.*

rules in terms of the Social Choice Function (SCF) such that players will play according to these rules. The balance of IDS resource consumption problem can be modelled using mechanism design theory with an objective function that depends on the private information of the players. In our case, the private information of the player is the cost of analysis which depends on the player's energy level. Here, the rational players select to deliver the untruthful or incomplete information about their preferences if that leads to individually better outcomes. The main goal of using mechanism design is to address this problem by designing incentives for players (nodes) to provide truthful information about their preferences over different outcomes and computing the optimal system-wide solution.

### 3.2 The Mechanism Model

We treat the IDS resource consumption problem as a game where the N mobile nodes are the agents/players. Each node plays by revealing its own private information (cost of analysis) which is based on the node's type. The type is drawn from each player's available type set. Each player selects his own strategy/type according to how much the node values the outcome. If the player's strategy is normal then the node reveals the true cost of analysis. In our case, if the node is elected then the cost of analysis is 0 since the node will not be the leader and hence there will be no cost to run the IDS. Payment is given in the form of reputation. Nodes that are not elected receive no payment. Note that, what the player usually seeks to maximize. It reflects the amount of benefits gained by player if he follows a specific type. Players might deviate from revealing the truthful valuation for the cost of analysis if that could lead to a better payoff. Therefore, our mechanism must be strategy-proof where truth-telling is the dominant strategy. To play the game, every node declares its corresponding cost of analysis where the cost vector C is the input of our mechanism. For each input vector, the mechanism calculates its corresponding output and a payment vector. Payments are used to motivate players to behave in accordance with the mechanism goals. In the following subsections, we will formulate the following components

1) Cost of analysis function: It is needed by the nodes to compute the valuation function.
2) Reputation system: It is needed to show how
a) Incentives are used once they are granted.
b) Misbehaving nodes are caught and punished.
3) Payment design: It is needed to design the amount of incentives that will be given to the nodes.

## 4 Proposed Method

### 4.1 Cluster Formation

In clustering the mobile nodes in a MANET are divided into different virtual groups, and they are allocated geographically adjacent into the same cluster according to some rules with different behaviours for nodes included in a cluster from those excluded from the cluster. Clustering is a network to achieve scalability in the presence of a large number of mobile nodes and high mobility. Under a cluster structure, mobile nodes may be assigned a different status or function, such as cluster head (CH), cluster gateway, or cluster member (CM). A cluster head normally serves as a local coordinator for its cluster, performing intra-cluster transmission arrangement, data forwarding, and so on.

Before CHs selection, we firstly divide the network into k equal regions according to the optimal cluster number. Cluster head only manages the data collected from the region and then relay the aggregated data to SN. Besides, neighbour nodes of SN will perform direct transmission to SN. After cluster formation, we assign a random initial energy level to each node. To balance the energy consumption levels, we use the initial energy levels to select the CH-candidate nodes. Upon being selected, each CH-candidate transmits a packet and advertises its ID and residual energy level. A CH-candidate monitors advertisements from others and defers from acting as a CH if a higher energy level is reported by another. Finally, candidate with the highest residual energy level will become CH. Other nodes in this region will become the member of this cluster.

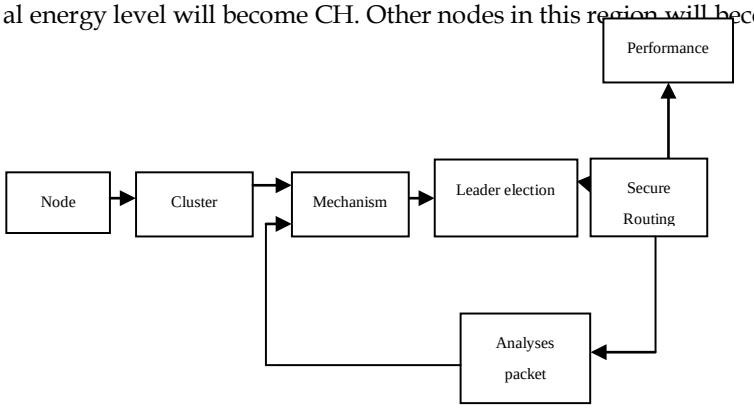


Fig 1. Block diagram of proposed system

### 4.2 Mechanism Design

The model guarantees that truth-telling is always the dominant strategy for every node during each election phase. On the other hand, to find the globally optimal weight based node as leaders.

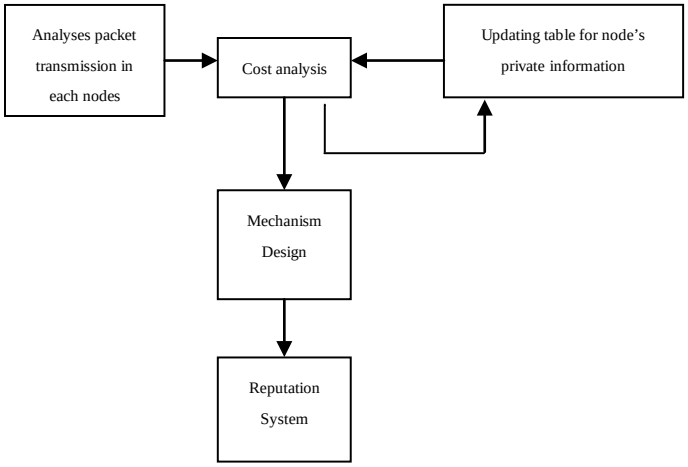


Fig 2. Mechanism design

In Fig.2 this mechanism design analyses the packet transmission and reception of the node, using this, it calculates the energy consumption of each node, through the mechanism calculates the current energy level of nodes in clusters. Using nodes energy level, this mechanism elect most cost efficient node as leader node.

### 4.3 Leader Election Module

Leader-election algorithm that helps to elect the most weight based leaders with less performance overhead compared to the network flooding model. We devise all the needed messages to establish the election mechanism taking into consideration cheating and presence of malicious nodes. Moreover, we consider the addition and removal of nodes to/from the network due to mobility reasons. The performance overhead is considered during the design of the given algorithm where computation, communication and storage overhead are derived.

Using the cost analysis function node's current energy level is calculated, we assume that each node has different energy level at different time interval which is consider as private information. We defined this mechanism to find a largest energy level node in the cluster. This model guarantees that truth-telling is always the dominant strategy for every node during each election phase. On the other hand to find the globally optimal weight based node as leaders.

To design the leader election algorithm, the following requirements are needed: (1) to protect all the nodes in a network, every node should be monitored by a leader. (2) To balance the resource consumption of service, the overall cost of analysis for protecting the whole network is minimized. To start a new election, the election algorithm uses four types of messages. Hello, used by every node to initiate the election process; Begin-Election, used to announce the cost of a node; Vote, sent by every node to elect a leader; Acknowledge, sent by the leader to broadcast its payment, and also as a confirmation of its leadership. It is unfair and unsafe way for one node be a leader forever ,so during the interval T-elect to enforce re-election .After completion of the particular duration all node go back to the initial stage and start new election process using above four messages.

### 4.4 Cost Analysis

During the design of the cost of analysis function, the following two problems arise: First, the energy level is considered as private and sensitive information .Second, if the cost of analysis function is designed only in terms of nodes energy level, then the nodes with the low energy level will not be able to perform cluster service. The cost of analysis is designed based on the energy value, the expected number of time slots that a node wants to stay alive in a cluster. Each node energy level is updated using below calculation

Current energy = last update of energy – no. of packets transmitted per node – energy consumption for running IDs.

The lifetime of a node can be divided into time-slots. Each node i is associated with an energy level, denoted by Ei, and the number of expected alive slots is denoted by nTi. Based on these requirements, each node i has a power factor PFi = Ei/nTi.

### 4.5 Secure Routing

The main drawback in MANET is lack of security. In this we using Diffie –Hellman key exchange protocol to improve the security .Through this we can able to reduce the overload and avoid time synchronization problem. Diffie–Hellman key exchange (D–H) is a specific method of exchanging keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish

a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. Diffie–Hellman establishes a shared secret that can be used for secret communications by exchanging data over a public network. In Diffie-Hellman key exchange both users select a common prime number and base number. Then both users select their separate secret keys and share the common shared key. So the security is high in this than the other key exchange techniques.

The following security services are provided for secure communication.

(1) Nodes authentication within the cluster

(2) Nodes communication within the cluster. It is divided into two cases. In the first case communication between the nodes within coverage range and in second case, the communication is carried out through the intermediate nodes i.e., nodes in out of coverage range.

(3) Cluster head shares it secret value to its entire member's.

(4) Communication between two nodes, which are located in different cluster.

## 5 Performance Evaluation

The main objective of simulation results is to study the effect of node selection for the life of all nodes. Besides, use the following metrics to evaluate algorithm against others: Percentage of alive nodes, energy level of nodes, percentage of leader node, average cluster size, maximum cluster size and number of single node clusters. The experiments have been conducted in both static and dynamic networks. Initially, randomly assign 60 to 100 joules to each node.

This model is able to balance the resource consumption in the presence of selfish nodes. Moreover, it is able to reduce single node clusters and also the maximum cluster size. Besides, it achieves more uniform clusters with less leader nodes.

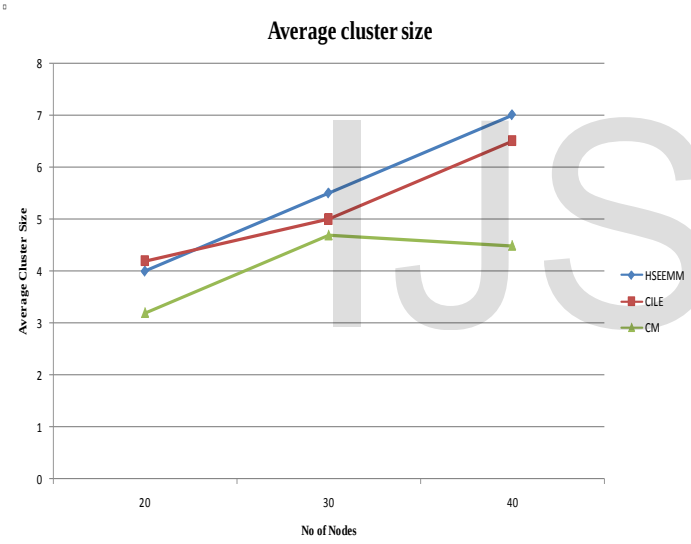




Fig 3. Average Cluster Size

In Fig.3 the average cluster size of this model is compared with CILE, and connectivity model for different number of nodes. This model provides higher average cluster size then the another two models, It reduce the communication overhead in cluster heads .

In Fig.4 this model is able to reduce the number of single node clusters as the density of node is increasing.

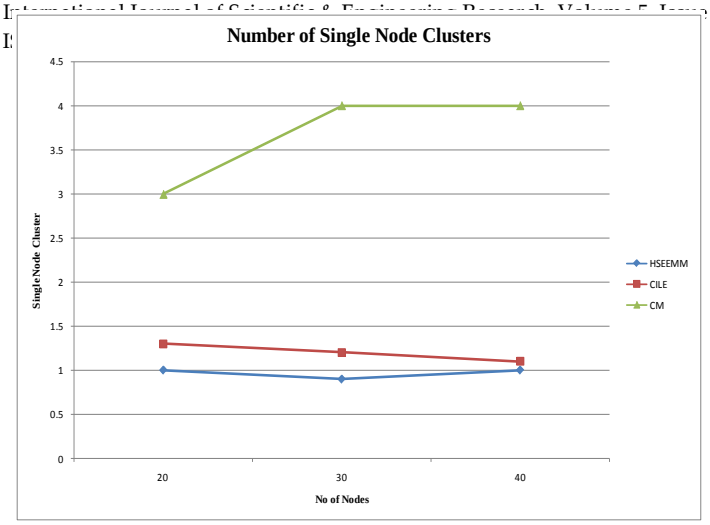


Fig 4. No of Single Node Clusters

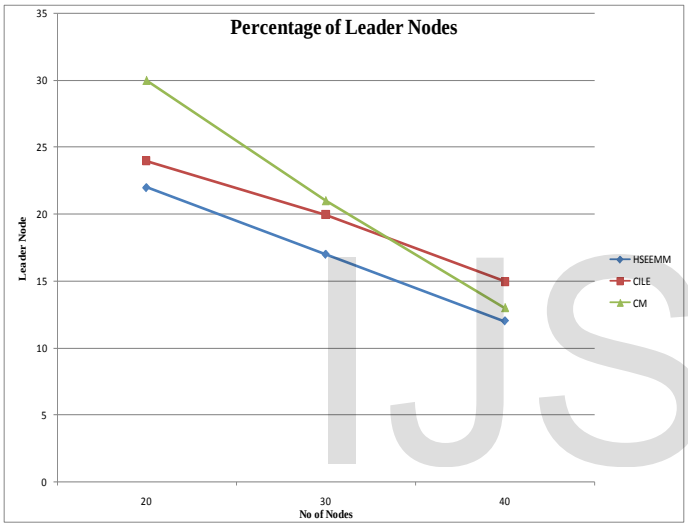




Fig 5. Percentage of Leader Nodes

In Fig.5 the Percentage of Leaders for this model is less compared to the connectivity and cluster independent leader election model. Less number of leader nodes in network reduces the energy consumption and increase the MANET life time.

## 6 Conclusion

The Unbalanced resource consumption in MANET and presence of selfish nodes are the two important problems in Mobile Adhoc Network. It is solved by using cluster formation algorithms and leader election mechanism. This model is able to prolong the life time of MANET, decrease the percentage of leader nodes, maximize the cluster size and data compression for secure routing, and energy consumption of nodes.

## References

[1] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabi Bhattacharya.Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET ,2011.

[2] Oussama Souihli, Mounir Frikha, and Mahmoud Ben Hamouda. Load-balancing in Manet shortest-path routing protocols. Ad Hoc Netw, 7(2):431–442, 2009.

[3] Gang Zhang, Xiaoyan Kuang, Jing Chen, and Yu Zhang. Design and implementation of a leader election algorithm in hierarchy mobile ad hoc network. In 2009 4th International Conference on Computer Science & Education, pages 263–268, 2009.

[4] M.Mizanur Rahman, M.Abdullah-Al-Wadud, and Oksam Chae. Performance analysis of leader election algorithms in mobile ad hoc networks. In IJCSNS International Journal of Computer Science and Network Security, February 2008.

[5] H.safa,Mirza.O ,Artail.H. A Dynamic Energy Efficient Clustering Algorithm for MANET.IEEE International Conference on Wireless and Mobile Computing, 2008.

[6] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya. A mechanism design-based multi-leader election scheme for intrusion detection in manet. In proc. of the IEEE Wireless Communications & Networking Conference (WCNC), 2008.
[7] Khaleel Ur Rahman Khan, Rafi U. Zaman, A. Venugopal Reddy, Kashifa Hafeez, and Tabassum Sultana. A hierarchical approach of integrating mobile ad hoc network and the internet. pages 1–4. 16th IEEE International Conference, 12-14 Dec 2008.
[8] F. Anjum and P. Mouchtaris. Security for Wireless Ad Hoc Networks.John Wiley & Sons. Inc., USA, 2007.
[9] H. Rifa-Pous and J. Herrera-Joancomarti. Secure dynamic Manet on-demand (sedymo) routing protocol. Pages 372 – 380, 29 May 2007.
[10] Chitra.R, Jayalakshmi.V, Jayashree.R, Keerthana.N, P.Karthik. Leader Election for IDwith ProlongedNetwork Life Time Using ELAR1-VAin MANET's,2007.
[11] K. Sun, P. Peng, P. Ning, and C. Wang. Secure distributed cluster formation in wireless sensor networks. In proc. of the IEEE Computer Security Applications Conference (ACSAC), 2006.
[12] M. Bechler, H.-J. Hofi, D. Kraftt, E Pmket, L. Wolf. A Cluster-Based Security Architecture for Ad Hoc Networks,2006.
[13] Salahuddin Mohammad Masum, Amin Ahsan Ali, and Mohammad Touhid youl Islam Bhuiyan. Asynchronous leader election in mobile ad hoc networks. Advanced Information Networking and Applications, International Conference on,2:827–831, 2006.
[14] Zongkai Yang, Qifei Zhang, Xu Du, and Linfeng Yuan. Location-based adaptive ad hoc routing (laar). Volume 2, page 1013 1017. IEEE International Symposium, 2005.
[15] Savio S.H. Tse and Francis C.M. Lau. An approximation solution for the 2- median problem on two-dimensional meshes. Advanced Information Networking and Applications, International Conference on, 2:457–460, 2005.
[16] Gilbert Chen, Joel W. Branch, and Boleslaw K. Szymanski. Local leader election, signal strength aware flooding, and routeless routing. In 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05) - Workshop 12, volume 13, page 2005.
[17] K. Chen and K. Nahrstedt. iPass: An incentive compatible auction scheme to enable packet forwarding service in MANET. In proc. Of the International Conference on Distributed Computing Systems, 2004.
[18] Ian D. Chakeres and Elizabeth M. Belding-Royer. Aodv routing protocol implementation design. In ICDCSW '04: Proceedings of the 24th International Conference on Distributed Computing Systems Workshops - W7: EC (ICDCSW'04), pages 698–703, Washington, DC, USA, 2004. IEEE Computer Society.
[19] A.Mishra, K. Nadkarni, and A. Patcha. Intrusion detection in wireless ad hoc networks. IEEE Wireless Communications, 11(1):48 – 60, 2004.
[20] Prince Samar, Marc R. Pearlman, and Zygmunt J. Haas. Independent zone routing: an adaptive hybrid routing framework for ad hoc wireless networks, IEEE/ACM Trans. Netw., 12(4):595–608, 2004.
[21] S. Vasudevan, J. Kurose, and D. Towsley. Design and analysis of a leader election algorithm for mobile ad hoc networks. In proc. of the IEEE International Conference on Network Protocols (ICNP), 2004.
[22] S. Vasudevan, B. DeCleene, N. Immerman, J. Kurose, and D. Towsley. Leader election algorithms for wireless ad hoc networks. In proc. Of the IEEE DARPA Information Survivability Conference and Exposition (DISCEX III), 2003.
[23] Tomas Johansson and Lenka Carr-Moty˘ckov´.On Clustering in Ad Hoc Networks.Division of Computer Science and Networking Lule°a University of Technology August 17, 2003.
[24] Tim Daniel Hollerung. Mobile ad-hoc networks based on wireless lan. In University of Paderborn, 2003.
[25] Dong-Hee Kown, Woo-Jae Kim, and Young-Joo Suh. Dong-hee kown, woo-jae kim,young-joo suh, performance comparisons of two on-demand ad hoc routing protocols in dynamic rate shifting wlans. Volume 1, page 512 516, May 2003.
[26] Gruber and S. Hogg. Experimental results with a gps and signal strength extended ad hoc routing protocol. Pages 710 – 718, 03 November 2003.
[27] O. Kachirski and R. Guha. Efficient intrusion detection using multiple sensors in wireless ad hoc networks. In proc. of the IEEE Hawaii International Conference on System Sciences (HICSS), 2003.
[28] Yuanzhu Peter Cheny, Arthur L. Liestmany, and Jiangchuan Liuz. Clustering Algorithms For Ad Hoc Wireless Networks,2002.
[29] S. Buchegger and J. L. Boudec. Performance analysis of the CONFIDANT protocol (cooperation of nodes - fairness in dynamic adhoc networks). In proc. of the ACM MOBIHOC, 2002.
[30] Charles E. Perkins and Elizabeth M. Royer. The ad hoc on-demand distance vector protocol. Pages 173–219, 2001.