International Journal of Computational Intelligence and Informatics, Vol. 1 : No. 4, January - March 2012

Energy Efficient and Secure Communication Protocol in MANET

G. Siva Kumar,
PG Scholar(Computer and Communication),
National Engineering College, Kovilpatti.
E-Mail: gsivakvp@gmail.com

***M. Kaliappan, **L. Jerart Julus,**
Assistant Professor, Dept of IT.,
National Engineering College, Kovilpatti.
**E-Mail: kalsrajan@yahoo.co.in*
***E-Mail: jerartjulus@gmail.com*

Abstract

Recent year a rapid development and widespread application of mobile ad hoc networks suffer from security attacks and privacy issues which dramatically impede their applications. To cope with the attacks, a large variety of intrusion detection techniques such as authentication, authorization, cryptographic protocols and key management schemes have been developed. Clustering methods allow fast connection, better routing and topology management of mobile ad hoc networks (MANET). This paper, we have introduced new mechanism called Energy Efficiency and Secure Communication Protocol (EESCP) is to divide the MANET into a set of 2-hop clusters where each node belongs to at least one cluster. The nodes in each cluster elect a leader node (cluster head) to serve as the IDS for the entire cluster. To balance the resource consumption weight based leader election model is used, which elected an optimal collection of leaders to minimize the overall resource consumption and obtaining secure communication using diffie-Hellman key exchange protocol.

Keywords: Security; Leader election; EESCP; Mobile adhoc networks.

1. Introduction

Mobile Ad hoc Networks have no fixed chokepoints /bottlenecks where Intrusion Detection Systems (IDSs) can be deployed [1], [2]. Hence, a node may need to run its own IDS and cooperate with others to ensure security, [3],[7]. This is very inefficient in terms of resource consumption since mobile nodes are energy-limited. The leader-IDs election process can be either random [8] or based connectivity model (CM) [9]. Both approaches aim to reduce the overall resource consumption of IDs in the network. However, we notice that nodes usually have different remaining resources at any given time, which should be taken into account by an election scheme [10]. In random model and connectivity index-based approach some nodes will die faster than others, leading to a loss in connectivity and potentially the partition of network. Although it is clearly desirable to balance the resource consumption of IDs among nodes, this objective is difficult to achieve since the resource level is the private information of a node. 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 and Omar Mirza, and et.al [4] 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 and Lenka Carr-Motyˇckov´a [5] have proposed a 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, jean-Yves Boudec [6] 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. Proposed Methodology

A. Clustering

Clustering is an important research topic for MANET because clustering makes it possible to guarantee basic levels of system performance, such as throughput and delay, in the presence mobility and a large number of mobile nodes. In a clustering scheme[12] the mobile nodes in a MANET are divided into different groups, and they are allocated geographically adjacent into the same cluster according to some rules with different behaviors for nodes included in a cluster from those excluded from

the cluster. Some clustering schemes may cause the cluster structure to be completely rebuilt over the network when some local events take place, e.g. the movement or "die" of a mobile node, resulting in some clusterhead re-election (re-clustering).

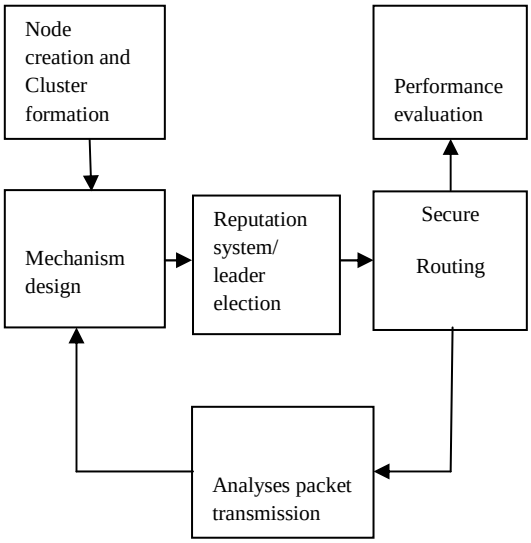

Figure1: Block diagram of proposed system

1) EESCP based clustering

The EESCP based cluster mechanism form the clusters with 2-hop neighboring nodes which is reduce the number of clusters and leader nodes. The node having highest energy of a cluster is called cluster head which is responsible for managing the cluster. A node in EESCP can be one of the following roles: (1) cluster head, (2) member node, (3) border node. One-hop neighbors of the cluster are called Member nodes. Border nodes are those nodes at the edge of the cluster (i.e., two hops away from the cluster head). In this mechanism we could achieve prolong the network life time and also reduce the routing overhead.

2) Setup Phase

Each node in a MANET starts as a free node and calculates its connectivity from their 2-hop radius nearest nodes in the network. After forming cluster higher connectivity node act as cluster head in the first time slot, then the nodes battery level is calculated and highest battery level node is selected as head.

3) Cluster Maintenance

In MANET, due to nodes mobility the cluster structure may change in every time, when a new cluster is formed, the 2-hop neighbor nodes inform their presence to cluster head, so that the cluster head can maintain the topological information of the cluster.

B. 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 cost-efficient node as leaders. This mechanism design [11] 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, EESCP mechanism elect most cost efficient node as leader node. Reputation system used to monitor the behavior of leader node and compares the leader nodes current energy level with predefined threshold value, using this threshold check we identify the leader node having enough energy to run IDs or not. If the leader node energy is less than a predefined threshold loader node exclude from the cluster service.

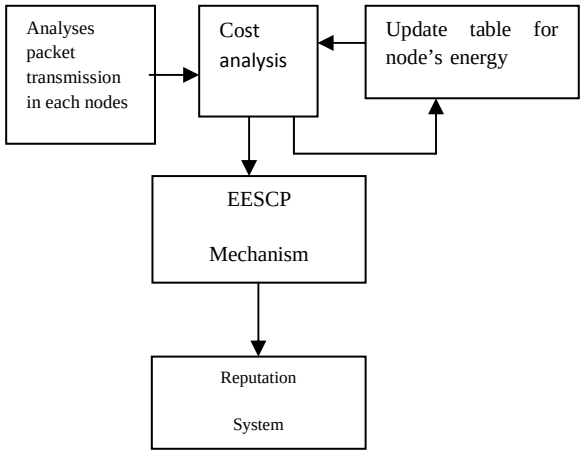

Figure2: Mechanism design

1) Cost of Analysis Function

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.

2) *Elect the highest energy node*

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 EESCP 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 cost-efficient node as leaders. 2-hop cluster has higher number of nodes compared to 1-hop cluster; it increases the computation time to finding highest energy level node in the cluster.

EESCP mechanism works like divide and conquer method, it decrease computation time.

Algorithm for Finding Largest Energy Level node in Cluster:

Step 1**:**
If (participation node's are even)
Split into two half's
Else
Round the first half of nodes into nearest maximum integer value, remaining nodes are placed in second half.

Step2: Repeat until n/2=0 (or) n/2=0.5=>1

Step3: Compare the node energy level its next node and low energy level node is not allowed to participate next round

Step4: Repeating step 3, In ((n/2) +1) th round we obtain highest energy level node in the network or cluster.

Assume Cluster has 10 nodes, fig3 shows, how the largest energy level node is selected.1 to 10 consider as node energy value.

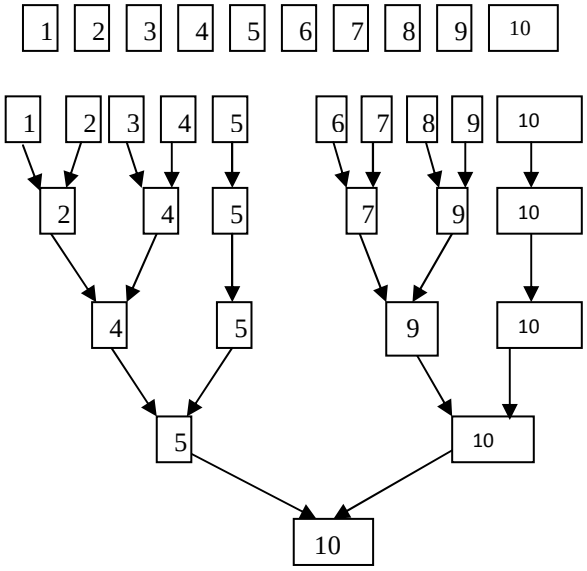

Figure3: Electing high energy node

3) Leader election algorithm

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 IDS 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. For describing the algorithm, we use the following notation:

• Service-table (k): The list of all ordinary nodes, those voted for the leader node k.

• Nodes energy level update-table(k): The reputation table of node k. Each node keeps the

• Leadernode(k): The ID of node k's leader. If node k is running its own IDS then the variable contains k. A boolean variable that sets to TRUE if node k is a leader and FALSE otherwise.

Algorithm for Initialize the election process:

if (received *Hello* from all neighbors)
then

Send *Begin-Election* (IDk, costk);
else if
(neighbors (k)=Ø)
then
Launch IDS.
end if
On expiration of T1, each node k checks whether it has received all the hash values from its neighbors. Some clusters have a single node so it does not receive Hello message from its neighbors, this algorithm allows the single node act as leader.

Algorithm for every node in the cluster sends vote message to highest energy level nodes:
if ($\forall$ n _ neighbor(k), $\exists$ i _ n : ci $\leq$ cn)
then
send Vote(IDk, IDi , costj_=i);
leadernode(k):= i;
end if

Begin-Election to verify the cost of analysis for all the nodes. Then node k calculates the least-cost value among its neighbors and sends *Vote* for node i as in Algorithm 2. The *Vote* message contains the ID_k of the source node, the ID_i of the proposed leader. Then node k sets node i as its leader in order to update later on its energy value. Time slot 2 computations are start to finding leader node.

Algorithm for the leader to broadcast its energy level and confirmation of its leadership:

Leader(i) := TRUE;
Compute energy, Pi;
$update_{service-table(i)}$;
$update_{reputation-table(i)}$;
Acknowledge = Pi + all the votes;
Send Acknowledge (i);
Launch IDS.

The *Acknowledge* message contains the energy level of nodes and the votes the leader received. The leader then launches its IDS.

C. Adding a new node

When a new node is added to the network, it either launches its own IDS or becomes an ordinary node of any leader node. To include a new node to the IDS service,

four messages are needed: Hello, Status, Join and Acknowledge. Hello is sent by a new node n to announce its presence in the network.

Algorithm for joining new node in cluster:

```
if (leader(k) = TRUE) then
        Status := Cost_k;
 else
        Status := leadernode(k);
 end if;
        send Status(k, n);
```

D. Removing a node

When a node is disconnected from the network due to many reasons; such as, mobility or battery depletion, then the neighbor nodes have to reconfigure the network.

Algorithm for remove the node from cluster:

```
 if (leadernode(k) = n)
then
        leadernode(k):= NULL;
        update_energy(k);
        send Begin − Election as in Algorithm 1;
 end if;
 if (leader(k) = TRUE) then
 if (n ∈ service(k)) then
        update_service();
 end if;
 end if;
```

4. Secure Routing

The main drawback in MANET is lack of security. In EESCP we using Diffie –Hellman key exchange protocol[13] to improve the security .Through this we can able to reduce the overload and avoid time synchronization problem. It uses two public known numbers: a prime number q and an integer α that is prime root of q. If two nodes A,B want to communicate ,node A select random integer value $X_A < q$ then computes $Y_A = \alpha^{X_A} \bmod q$.

Similarly node B selects X_B and computes Y_B In each node X value is kept as private value and Y value broadcasted publicly, the node A computes key as $K=(Y_B)^{X_A} \bmod q$ and user B computes the key as $K=(Y_A)^{X_B} \bmod q$. This algorithm produced identical result for two nodes which exchanges a secret values.

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) Clusterhead 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 IDS on the life of all nodes. To show the negative impact of selfish node, conducted two experiments: Time taken for the first node to die and percentage of packet analysis. 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.

A. Simulation Environment

To implement the models, we modify the energy model to measure the effect of running IDS. We assume that the energy required for running the IDS for one time slot as 10 joules. We ignore the energy required to live and transmit packets to capture the silent aspect of the problem. We set the transmission radius of each node to 200 meters. Two nodes are considered as neighbors if their Euclidean distance is less than or equal to 200 meters.

Parameter	Value
Simulation time	350secs
Simulation area	500*500
Number of nodes	20,30,40,50
Transmission range	200m
Movement model	Random waypoint model
Pause time	200sec
Traffic type	CBR/UDP
Packet rate	4 packets/sec
T-elect	20sec

Two nodes are considered as neighbors if their Euclidean distance is less than or equal to 200 meters . Besides, we deploy different number of nodes, which varies from 20 to 50 in an area of 500 × 500 square meters. It helps us to measure the performance of the nodes from sparse networks to dense networks.

6. Result

Table1: Energy Level Of nodes

Models	No.of nodes								
	1	2	3	4	5	6	7	8	9
CM	17	0	0	78	0	50	78	0	0
CILE	24	24	25	26	26	27	27	26	27
EESCP	26	26	27	28	28	28	28	27	28

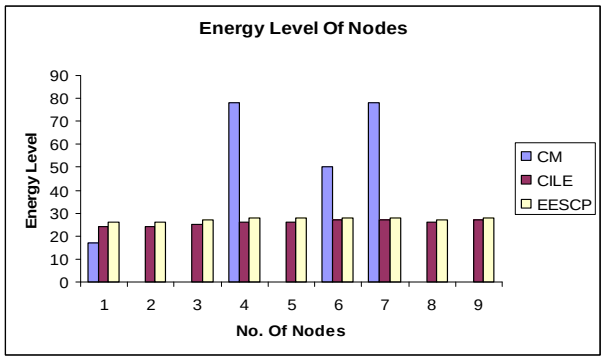

Figure4: Energy Level Of nodes

EESCP model is able to balance the resource consumption among all nodes. Comparing Connectivity and Cluster independent leader election model (CILE).

Table2: Percentage of Leader node

Models	No.of. nodes			
	20	30	40	50
CM	3	4	4	4
CILE	1.2	1.1	1	0.9
EESCP	1	0.9	0.9	0.8

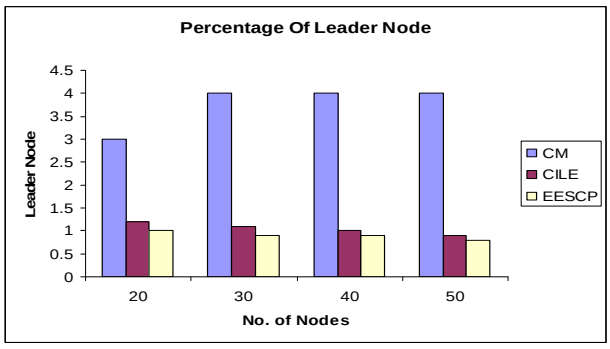

Figure5: Percentage of Leader node

The Percentage of Leaders for EESCP model is less compared to the connectivity and cluster independent leader election model.

Table3: Average Cluster Size

Models	No.of. nodes			
	20	30	40	50
CM	3.2	5	5	5
CILE	4.2	5.4	7.8	8
EESCP	4	5.6	8	8.2

Compare the average cluster size of CILE, EESCP and connectivity model for different number of nodes, EESCP model provides higher average cluster size then another two models.

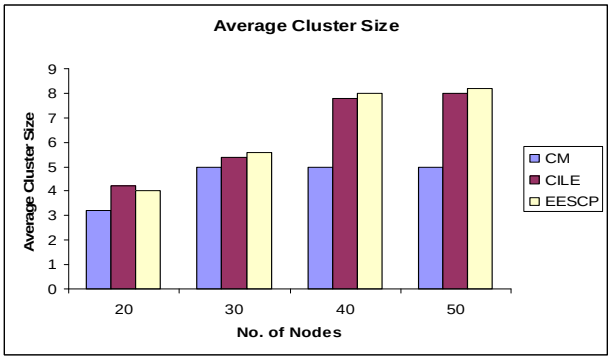

Figure6: Average Cluster Size

Table4: Computation delay

Models	No.of. nodes			
	5	10	15	20
CILE	5	10	15	20
EESCP	4	6	9	11

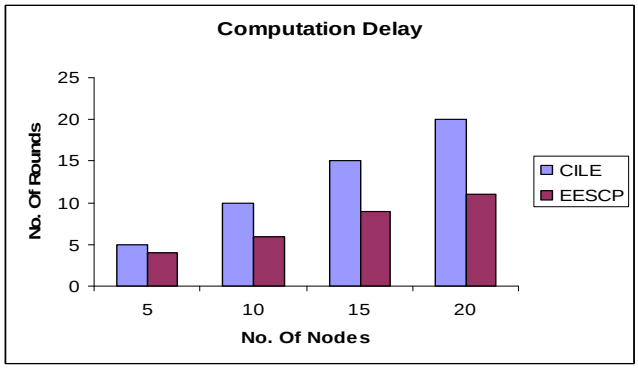

Figure7: Computation delay

Compare the computation delay of CILE, EESCP for different number of nodes, EESCP model find a high energy level node in less number round, so this model reduce the computation delay.

5. Conclusion

The Unbalanced resource consumption of IDs in MANET and presence of selfish nodes are the two important problems in Mobile Adhoc Network. It is solved by using EESCP based 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 decreases the computation delay.

References

[1] F. Anjum and P. Mouchtaris. Security for Wireless Ad Hoc Networks. John Wiley & Sons. Inc., USA, 2007.

[2] P. Brutch and C. Ko. Challenges in intrusion detection for wireless adhoc networks. In *proc. of the IEEE Symposium on Applications and the Internet (SAINT) Workshop*, 2003.

[3] P. Ning and K. Sun. How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols. In *proc. of the IEEE Information Assurance Workshop*, 2003.

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

[5] Tomas Johansson and LenkaMotyˇckov´.On Clustering in Ad Hoc Networks. *Division of Computer Science and Networking Lule°a University of Technology August 17, 2003*.

[6] 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*.

[7] T. Anantvalee and J. Wu. A survey on intrusion detection in mobile ad hoc networks. *Wireless/Mobile Network Security, 2006*.

[8] Y. Huang and W. Lee. A cooperative intrusion detection system for ad hoc networks. In *proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2003.

[9] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. *In proc. of the ACM International Conference on Mobile Computing and Networking (MobiCom), 2000.*

[10] L. Hurwicz and S. Reiter. Designing Economic Mechanisms. *Cambridge University Press, 1st edition, 2008.*

[11] *M.H.Guo,H.T.Liaw ,D.J.Deng H.C.Chao.Cluster based secure communication mechanism in wireless adhoc networks.In proc* of the IET Information Security .2010.

[12] P. Krishna, N. H. Vaidya, M. Chatterjee, and D. K. Pradhan. A clusterbased approach for routing in dynamic networks. *In proc. of the ACM SIGCOMM Computer Communication Review, 1997.*

[13] Ayan Mahalanobies.*Diffie-Hellman Key Exchange Protocol*,its Generalization and Nilpotent Groups Florida.. Atlantic…University, Augest 2005.