AN ENERGY EFFICIENT LEADER ELECTION MODEL IN MANET USING MECHANISM DESIGN THEORY

[1] K. Amsaveni, [2] G.Siva Kumar
[1]Assistant Professor, [2]Assistant Professor,
[1]Computer Science and Engineering,
[1]PSR Engineering College, Sivakasi, India.

Abstract: A Mobile Ad-hoc network (MANET) is formed when group of mobile nodes collaborate between them to communicate through wireless links in the absence of the fixed infrastructure and any centralized control. Clustering is an important approach in ad hoc networks for achieving scalability, ease of routing, basic performance guarantees such as throughput and delay, in the presence of large number of mobile nodes and high mobility. Due to dynamic nature and lack of centralized monitoring points, these networks are highly vulnerable to attacks. Intrusion detection systems (IDS) provide audit and monitoring capabilities that offer the local security to a node and help to perceive the specific trust level of other nodes. An IDS is also used to deal with selfish nodes that do not provide services to other nodes while at the same time benefiting from the resources of those nodes. In this paper, we propose a solution to selfish nodes based on Mechanism design theory. It is based on Vickers, Clarke, rooves (VCG) model to ensure truth-telling to be the dominant strategy for every node and also we proposed an On-Demand Energy based Leader Election Algorithm (OELEA), it can lead to globally optimal leader election in a cluster in which the node with most remaining resources is elected as leader in order to balance the resource consumption among all nodes and to prolong the lifetime of the network.

***IndexTerms* – Intrusion,Mechanism Design,Cluster,leader Election.**

I.INTRODUCTION:

A MANET is a collection of mobile nodes that communicate via message passing over wireless links. It can deploy in an environment, where the existence of network infrastructure or centralized administration is not present. Adhoc networks may also work in multihop environment whereas Cellular networks are single-hop wireless networks so an ad hoc network can reach the destination in a multihop manner. The mobile nodes within a transmission range can communicate directly. Due to the characteristics of wireless ad-hoc networks, including mobility, communication and recourse constraints leader election in mobile ad-hoc is a challenging problem. Indeed, several algorithms have been proposed to solve this problem. But most of them can be characterized as extrema-finding algorithms in which nodes are assumes to have a unique ID numbers, and the leader which is elected is simply that node which has the largest ID number. A cluster denotes a logical region of a MANET where nodes are highly connected with each other. In a clustering scheme the mobile nodes in a MANET are divided into different number of groups, and they are allocated geographically adjacent into the same cluster according to some rules . Each cluster consist of cluster head, cluster gateway and cluster member. A cluster head normally serves as a local coordinator or monitor for its cluster. The cluster head performs intra-cluster transmission arrangement, data forwarding, and so on.

A cluster gateway is a non-cluster head node it is usually called an ordinary node with inter-cluster links, so it can access neighboring clusters via the gateway node and forward information between clusters. A cluster member is a non-cluster head node without any inter-cluster links.

The classical statement of the leader election problem is to eventually elect a unique leader from a set of nodes. In mobile ad hoc networks the elected leader must be specialized on two important ways. First, it must tolerate arbitrary, concurrent topological changes and should eventually terminate electing unique leader second, elected leader node must be the most valued-node among all other nodes within a cluster or connected component the value of a node refers the performance related characteristic such as remaining battery life, minimum average distance to other nodes or computation capabilities.

Hence a leader node must take all the system related and security issues into consideration in this paper, we discuss the leader election model for intrusion detection with the purpose of examining all the properties depicted above.

II. RELATED WORKS

Leader election is an extensively studied problem for networks with static topologies. But, few algorithms exist to implement leader election for mobile ad hoc networks.

Anantvalee T. and Jie Wu have proposed [1] a survey on intrusion detection in mobile ad hoc networks. In Stand-alone Intrusion Detection Systems architecture, every decision made is based only on information collected at its own node, since there is no cooperation among nodes in the network. A watchdog identifies the misbehaving nodes by eavesdropping on the transmission of the next hop.Pathrater performs the calculation of the\path metric" for each path. The number of new attacks should be detected before they can do any harm to the systems or data[3].Attackers may try to attack the IDS system itself

K-P. Hatzis, G-P. Pentaris presented [4] two categories of algorithm, namely Compulsory protocols and Non-Compulsary. Non-Compulsory protocols (which do not affect the motion of nodes) and Compulsory protocols (which determine the motion of some or all of the nodes). Since the Non-Compulsory protocols do not affect the motion of the nodes each mobile node must move in order to exchange information. If nodes fail to meet the requirement, the protocol may not elect a unique leader. The mobile nodes are assumed to move in such a way that the number of elector-nodes that participate in protocol execution decreases with time. When there is only one participant left, that node becomes the leader. In order to elect a unique leader the Compulsory protocols require nodes to perform a random walk on the graph.

N.Malpani and N.Vaidya [2] proposed two leader election algorithms namely SEFA and SPLEA, which use a round-based hierarchy-building approach towards leader election. The Secure Extrema Finding Algorithm (SEFA) assumes that all elector-nodes exchange a single, evaluation function that returns the same "value" at any elector-node when applied to a given candidate-node. A candidate-node's identifier (name), battery life, or certified level-of-trust within the system are examples of values for which all nodes might well hold such a common view of a candidate node. In Secure Preference-based Leader Election Algorithm (SPLEA) individual utility functions at each elector-node determine the elector-node's preference for a given candidate-node; SPLEA serves to aggregate individual elector-node preferences into a single, system-wide choice of a leader. In both algorithms, any node detecting failure of leader circulates a message declaring itself as leader over the network.

T.J. Giuli and Mary Baker proposed watchdog method [12] to detect the misbehaving nodes in the MANET. It identifies the misbehaving nodes by eavesdropping on the transmission of next hop. The algorithms presented in [13], [14] and [15] are based on a routing algorithm called TORA [16] wherein nodes adjust a locally maintained variable, called the height, to point to the leader, in a decrementing manner over a Directed Acyclic Graph (DAG). These algorithms use the mechanisms in TORA to detect partitions, with the node detecting a partition being elected as a leader.

K.Hatzis and E.Royer have proposed Leader election algorithms for mobile ad hoc networks [6, 9].The proposed algorithms do not consider security issues and are not extreme-finding algorithms. Also, most of the leader election algorithms for mobile ad hoc networks elect a "random" leader and hence are not extreme-finding Security are also of particular concern in any wireless environment. Existing leader-election algorithms implicitly assume complete trust among the nodes participating in the leader election process, and consequently are vulnerable to a variety of attacks[11].

III. OUR CONTRIBUTION

In order to elect an optimal leader, the mobile nodes are grouped based on Vote based clustering algorithm [8] which is based on two factors neighbouring nodes and remaining battery time of every mobile host (MH).Each MH has a unique identifier (ID) number, which is a positive integer. The basic information inside the network is Hello message, which is transmitted in the common channel. Making use of node location information and power information, this algorithm introduces the concept of "vote". Using Hello messages each node is grouped into a particular cluster.

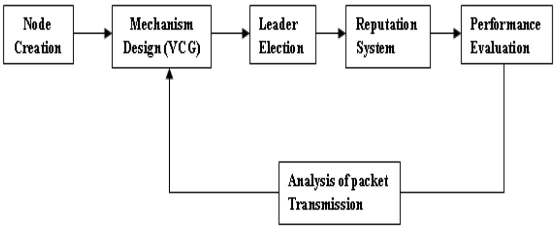

Fig: 3.1 Block Diagram of proposed method

Then it follows the classical mechanism design theory based on VCG model which guarantees that truth telling is always a dominant strategy of every node during each election process. Then the reputation system[10,7] is involved to motivate the nodes to behave normally in every election round. It can be used to determine whom to trust. The trust value is obtained from its neighboring nodes in the form of vote. A punishment system is involved to prevent nodes from behaving selfishly after the election. The reputation values of the Misbehaving nodes are decreased as a punishment. We proposed an On-Demand Energy based Leader Election Algorithm that helps to elect the most cost-efficient leaders to balance the overall resource consumption among all nodes in a cluster.

3.1 Mechanism Design Theory

Mechanism design theory [6] uses game theory tools to achieve a desired goal. Mechanism design allows us to define the game in such a way that the outcome of the game, known as the social choice function (SCF), will be played by independent players according to the rules set by the mechanism designer. We define selfish node as an economically rational node whose objective is to maximize its benefits (payoffs). The objective of minimizing the global cost of analysis while serving all the nodes can be expressed by the following Social Choice Function (SCF):

$$\text{SCF=S(C)} = \min \sum_{k\varepsilon N} c_k \cdot \left(\sum_{i\varepsilon N} vt_k\left(C,i\right) \cdot B \right)$$

In our model, we consider MANET as an undirected graph G = (N,L) where N is the set of nodes and L is the set of bidirectional links. We denote the cost of analysis vector as C =(c_1, c_2 . . . . c_n), where n is the number of nodes in N. We denote the election process as a function $vt_k(C,i)$, where $vt_k(C, i) = 1$ if a node i votes for a node k; $vt_k(C, i) = 0$, otherwise. We assume that each elected leader allocates the same budget B (in the number of packets) for each node that has voted for it. Knowing that the total budget will be distributed among all the voting nodes according to their reputation.

The balance of IDS resource consumption problem can be modeled 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. This mechanism analysis the packet transmission and reception of node, it calculates the energy consumption of each node and the current energy level of nodes in clusters. Using nodes energy level, VCG mechanism elect most cost efficient node as leader node. Therefore, incentives must be given to nodes to motivate them in cooperating. Incentives are provided to the node based on its reputation. Reputation (R) is used to decide whom to trust and motivate nodes to reveal truthfully their private information about their cost of analysis. The reputation of node i is denoted by Ri. This is indicated by the percentage of sampling

$$\text{PS} = \frac{R_i}{\sum_{i=0}^{N} R_i}$$

The cost function aggregates the cost of energy used to transmit and receive traffic, cost of collecting traffic, current battery and computational (CPU and memory) level. An elected leader should divide the corresponding node's sampling budget among node's incoming-links to increase the probability of detection. This model guarantees that truth telling is always dominant strategy for every node during each election phase also to find the globally optimal cost-efficient node as leaders.

3.2 On-Demand Energy based Leader Election Algorithm (OELEA)

The On-Demand Energy based Leader Election Algorithm aims to maintain stability of the network and facilitates the optimal operation of medium access control protocol. The assignment of weight to a mobile node is the combined effect of several system parameters like ideal node degree, degree difference, transmission power, energy and mobility. The advantage of this clustering scheme is the flexibility of adjusting the weighting factors for each system parameter to make it suitable for different scenarios. The procedure for cluster head election is as follows:

Step 1: Calculate the degree difference Du, Du = |nu-N| where nu is the number of neighbors of a mobile node u and N is the number of nodes that a cluster head can handle ideally. It is done to ensure efficient MAC functioning, as it is desirable for a cluster head to handle up to a predefined threshold (Td)

Step 2: Obtain the number of nodes (N_T) whose remaining energy level (E) exceeds the predefined threshold (E > Td). Then obtain a single node (N_u) from a set of nodes.

N_u = Max (N_T)
E = E_I – E_c

Where E_I –Initial Energy and E_c –Consumed Energy

Step 3: Compute the sum of the distances Su, with all the neighbors for every mobile node.

Step 4: Measure the mobility Mu, of every node by computing its average speed until the current time T as:

$$M = \frac{1}{T}\sum_{i=1}^{T} \sqrt{(X_t - X_{t-1}) + (Y_t - Y_{t-1})}$$

Where, (Xt, Yt) and (Xt-1,Yt-1) are the coordinates of the node u at time t and t-1 respectively.

Step 5: Compute the cluster head serving time Tu, which is the total time that a node u acts as a cluster head and it is measured by taking into the consideration of the drainage of node's battery power.

Step 6: Calculate the combined weight Cu, for each node u as:

$$C\,u = w_1 D_u + w_2 S_u + w_3 M_u + w_4 N_u$$

Where w1, w2, w3 and w4 are arbitrarily chosen weighting factors for the corresponding system parameters that satisfies the following condition:

$$\sum_{i=1}^{4} W_i = 1$$

Step 7: Elect the smallest Cu as cluster head and repeat steps 2 to 7 for the remaining nodes in $N_{T.}$

Step 8: Repeat the above steps for the remaining nodes in the cluster.

IV. RESULTS AND DISCUSSIONS

We evaluate the performance of our model (OELEA) with respect to connectivity model. We simulate the schemes using Network Simulator 2 (NS2).
The nodes randomly moves according to the Random Waypoint Mobility Model with different number of nodes varies from 20 to 50.

The main objective of our simulation results is to study the effect of node selection for IDS on the life of all nodes. To identify the false positive impact of selfish node, we conducted two experiments: Time taken for the first node to die and percentage of packet analysis. The following performance metrics are used to evaluate our algorithm against Connectivity Model (CM): percentage of leader node, average cluster size, maximum cluster size, and number of single-node clusters.

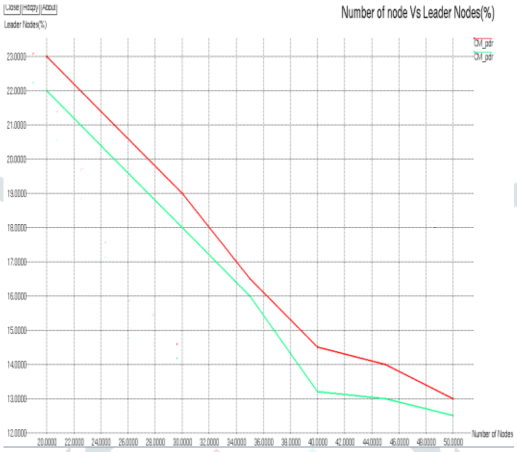

Fig: 4.1 Percentage of Leader Node

Fig 4.1 compares the average cluster size of (Cluster Dependent Leader Election) CDLE and (Connectivity Model) CM for different number of nodes, The CDLE model provides higher average cluster size, and this proves that our model is able to uniformly distribute the load of the leaders.

Fig. 4.2 shows the percentage of the leader nodes which compares both CM and CDLE model. The percentage of leaders for CDLE model is less as compared to those of the connectivity model that saves the energy of nodes. It decreases the percentage of leader node as the number of node increases.

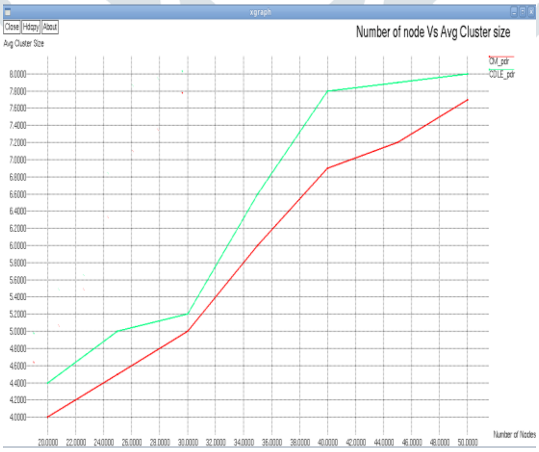

Fig: 4.2 Average cluster size

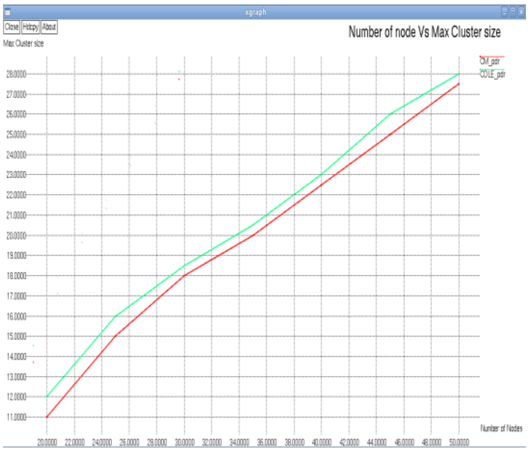

Fig 4.3 Size of maximum cluster

Fig 4.3 illustrates the size of the maximum cluster. The maximum cluster size for both models is increasing with the number of nodes. The maximum cluster size is slightly high for OELEA. This could also improve the detection probability since more number of packets are analyzed per node compared to the other model.

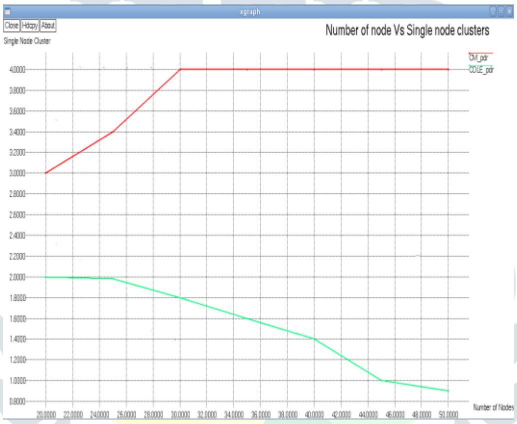

Fig 4.4 Number of single-node clusters

Fig 4.4 shows that our model is able to reduce the number of single-node clusters as the density of nodes is increasing.

V.CONCLUSION

In this paper, we proposed an On-Demand Energy based Leader Election Algorithm in which the cost efficient node has identified and elected as a leader. For the purpose security to both the leader and selfish nodes, VCG mechanism has employed which ensures that every node reveals its truthful information. Thus the proposed schemes will prolong the lifetime of MANET and balance the resource consumption among all nodes. Moreover, we are able to decrease the percentage of leaders, single-node clusters, and maximum cluster size, and increase the average cluster size. These properties allow us to improve the detection service.

VI. REFERENCES

[1] T. Anantvalee and J. Wu, " A Survey on Intrusion Detection in Mobile Ad Hoc Networks, " Wireless/Mobile Network Security, Springer, 2006.

[2] N. Malpani, J-L. Welch, and N. Vaidya, "Leader election algorithms for mobile ad hoc networks", Proceedings of the 4th International Workshop on Discrete Algorithms and Methods for MobileComputing and Communications, August 2000, pp. 96–103.

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

[4] K-P. Hatzis, G-P. Pentaris, P-G. Spirakis, V-T. Tampakas, and R. B.Tan, "Fundamental control algorithms in mobile networks", Proceeding of the 11th Annual ACM Symposium on Parallel Algorithms and Architectures, March 1999, pp. 251–260.

[5] S. Basagni, "Distributed Clustering for Ad Hoc Networks, "Proc. IEEE Int ' l Symp, Parallel Architectures, Algorithms, and Networks (ISPAN), 1999.

[6] L. Anderegg and S. Eidenbenz, "Ad Hoc-VCG: A Truthful and Cost-EfficientSelfish Agents," Proc. ACM MobiCom,2003.

[7] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on Dependable and Secure Computing, vol. 99, no. 1, 2008.

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

[9] E. Royer and C. Perkins. Multicast Operations of the Ad Hoc On-Demand Distance Vector Routing Protocol. In Proceedings of Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM),pages 207-218, August 15-20, 1999.

[10]T. Sakthivel, S.Vijaybhanu and R.M.Chandrasekaran"A Novel Leader based Reputation Approach for Mobile Ad Hoc Networks"International Journal of Computer Applications, vol 47, June 2012.

[11] S. Gwalani, K. Srinivasan, G. Vigna, E.M. Beding - Royer, and R. Kemmerer, " An Intrusion Detection Tool for AODV-Based Ad Hoc Wireless Networks, " Proc. IEEE Computer Security Applications Conf. (CSAC), 2003.

[12] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks" ACM proceedings of the 6th annual international conference on mobile computing and networking, pp. 255- 265, 2000.

[13] N. Malpani, J-L. Welch, and N. Vaidya, "Leader election algorithms for mobile ad hoc networks", Proceedings of the 4th International Workshopon Discrete Algorithms and Methods for Mobile Computing and Communications, August 2000, pp. 96–103.

[14] A. Velayutham and S. Chaudhuri, "Analysis of a leader election algorithm for mobile ad hoc networks". Technical report, Iowa State University, 2003.

[15] A. Derhab and N. Badache, "A self-stabilizing leader election algorithm in highly dynamic ad hoc mobile networks", IEEE Transactions on Parallel and Distributed Systems, vol. 19, no. 7, 2008, pp. 926–939.

[16] V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks", Proceeding of the 16th IEEE INFOCOM, April 1997, pp. 1405–1413.

L. Anderegg and S. Eidenbenz, "Ad Hoc-VCG: A Truthful and Cost-EfficientSelfish Agents," Proc. ACM MobiCom,2003.