Leader Election for ID with Prolonged Network Life Time Using ELAR1-VA in MANETs

[1]Chitra.R, [2]Jayalakshmi.V, [3]Jayashree.R, [4]Keerthana.N, [5]P.Karthik

[1,2,3,4] Students IV ECE, SNS College of Engineering, Coimbatore.
[5] Assistant Professor, SNS College of Engineering, Coimbatore.

Abstract- The Leader election process is done in the presence of selfish nodes for intrusion detection in mobile ad hoc networks (MANETs). The leader-IDS election process can be either random or based on the connectivity model. Unfortunately, with the random model, each node is equally likely to be elected regardless of its remaining resources. The connectivity index-based approach elects a node with a high degree of connectivity even though the node may have little resources left. Due to limited battery power nodes die out early and affect the network lifetime.

More specifically, the solution provides nodes with incentives in the form of reputations in order to encourage nodes to honestly participate in the election process. The amount of incentives is based on truth-telling dominant strategy for any node. To address the optimal election issue, we develop a series of local election algorithms that can lead to globally optimal election results with a low cost. We also enhanced our system by focusing on increasing energy efficiency of MANET. Due to limited battery power nodes die out early and affect the network lifetime. To make network energy efficient, we have modified position based Location Aided Routing (LAR1) for energy conservation in MANET. The proposed protocol is known as Variable Range Energy aware Location Aided Routing (ELAR1-VAR). The proposed scheme controls the transmission power of a node according to the distance between the nodes. It also includes energy information on route request packet and selects the energy efficient path to route data packets. ELAR1-VAR protocol improves the network lifetime by reducing energy consumption by 20% for dense and mobile network while maintaining the packet delivery ratio above 90%.

I. INTRUSION DETECTION IN MANET

2.1 LEADER ELECTION MECHANISM

In this section, leader election mechanism for truthfully electing the leader nodes is proposed.

2.2.1 Mechanism Design Background
2.2.2 Mechanism Model
2.2.3 Fairness and Privacy
2.2.4 Reputation System Model

Payment design in the form of reputation is illustrated in Fig 3.1
(1) Motivate nodes to behave normally.
(2) Punish the misbehaving nodes.

Moreover, it can be used to determine whom to trust. To motivate the nodes in behaving normally in every election round, relate the cluster's services to nodes' reputation. This will create a competition environment that motivates the nodes to behave normally by saying the truth. To enforce this mechanism, a punishment system is needed to prevent nodes from behaving selfishly after the election.

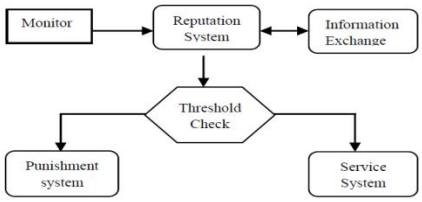


Fig 3.1 Reputation System Model

Misbehaving nodes are punished by decreasing their reputation and consequently are excluded from the cluster services if the reputation is less than a predefined threshold. As an extension to our model, reputation system is extending to include different sources of information such as routing and key distribution with different assigned weights. Figure shows the abstract model of the reputation system where each node has the following components:

Monitor or Watchdog

It is used to monitor the behaviour of the elected leader. To reduce the overall resource consumption, a set of nodes are randomly elected, known as checkers, to perform the monitoring process. The selected checkers mirror a small portion of the computation done by the leader so the checkers can tell whether the leader is actually carrying out its duty. The checkers are cooperative because the amount of computation they conduct for monitoring the leader only amounts to a marginal resource consumption, which is dominated by the benefit of receiving intrusion detection service from the leader.

Information Exchange

It includes two types of information sharing:
(1) The exchange of reputation with other nodes in other clusters (i.e., for services purposes).
(2) To reduce the false positive rate, the checkers will exchange information about the behaviour of the leader to make decision about the leader's behaviour.

Reputation System

It is defined in the form of a table that contains the *ID* of other nodes and their respective reputation R. The node that has the highest reputation can be considered as the most trusted node and is given priority in the cluster's services. Therefore, the rational nodes are motivated to increase their reputation value by participating in the leader election.

Threshold Check

It has two main purposes:

(1) To verify whether nodes reputation is greater than a predefined threshold. If the result is true then nodes services are offered according to nodes reputation.

(2) To verify whether a leader's behaviour exceeds a predefined misbehaving threshold. According to the result, the punishment system is called.

3.4 CILE Payment Design

In Fig 3.2 Cluster Independent Leader Election (CILE), each node must be monitored by a leader node that will analyze the packets for other ordinary nodes. Based on the cost of analysis vector C, nodes will cooperate to elect a set of leader nodes that will be able to analyze the traffic across the whole network and handle the monitoring process.

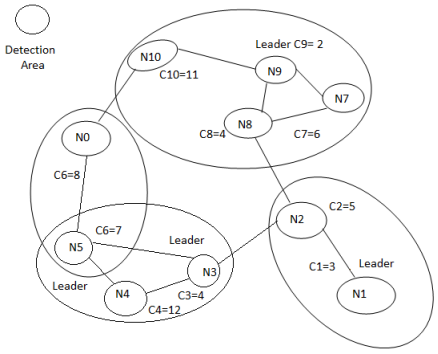


Fig 3.2 Example of Leader Election

This increases the efficiency and balances the resource consumption of IDS in the network. This mechanism provides payment to the elected leaders for serving others(i.e offering the detection service). The payment is based on a per-packet price that depends on the number of votes the elected nodes get. The nodes that do not get any vote from

3.5 CDLE Payment Design

In the whole network is divided into a set of clusters where a set of 1-hop neighbour nodes forms a cluster. Here, use the scheme of to cluster the nodes into 1-hop clusters. Each cluster then independently elects a leader among all the nodes to handle the monitoring process based on nodes' analysis cost. Main objective is to find the most cost-efficient set of leaders that handle the detection process for the whole network. Like CILE, CDLE provides payment to the elected node and the payment is based on a per-packet price that depends on the number of votes the elected node gets. Finally, selfish nodes might misbehave after election, which motivates us to select random checkers to ensure a catch-and-punish scheme in order to motivate an elected node to be faithful during the detection process. Using the following equation 4 and 5 design of payment, truth telling is the dominant strategy,

$$Pk = \sum_{i \in N} vt_k(C, i)\, B\rho_k \qquad (4)$$

$$\rho_k = min \sum_{j \in -nk} v_j\left(\theta_j, o(\theta_j, \theta_{-j})\right) \qquad (5)$$

According to the standard notation in mechanism design, the second best price is the simplest form of VCG mechanism. Here, $\sum_{j \in -n_k} v_j(\theta_j, o(\theta_j, \theta_{-j}))$ denotes the best cost excluding n_k. This is because nodes in the cluster have to select one node from the same cluster to be a leader. Unlike CILE where nodes can vote to its one-hop neighbour and then clusters are formed.

3.6 SECURITY ANALYSIS OF THE MECHANISM DESIGN

The main objective of the mechanism is to motivate selfish nodes and enforce them to behave normally during and after the election process.

3.6.1 Presence of Selfish Nodes

In Fig 3.3 the misbehaving leader can be catch and punish by the checker. A caught misbehaving leader will be punished by receiving a negative payment. Thus, it discourages any elected node from not carrying out its responsibility. Now, it can conclude that the mechanism is truthful and it guarantees a fair election of the most cost-efficient leader.

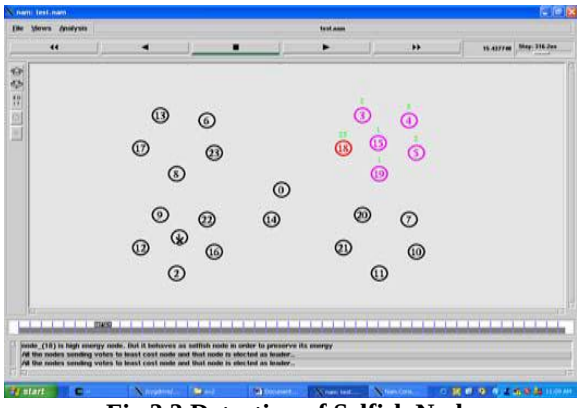


Fig 3.3 Detection of Selfish Node

3.6.2 Presence of Malicious Nodes

A malicious node can disrupt the election algorithm by claiming a fake low cost in order to be elected as a leader. Once elected, the node does not provide IDS services, which eases the job of intruders. To catch and punish a misbehaving leader who does not serve others after being elected, a decentralized catch and-punish mechanism are proposed using random checker nodes to monitor the behaviour of the leader. Although not repeated here, this scheme can certainly be applied here to the malicious nodes by catching and excluding them from the network. Due to the presence of checkers, a malicious node has no incentive to become a leader since it will be caught and punished by the checkers.

After a leader is caught misbehaving, it will be punished by receiving a negative reputation and is consequently excluded from future services of the cluster. Thus, the mechanism is still valid even in the presence of a malicious node.

3.6.3Adding a node

A new node has been added to the IDS service is shown in the Fig 3.4. For including a new node to the IDS service, four messages are needed: Hello, Join, status and Acknowledge. Hello is used to announce its presence in the network. After receiving the Hello message, all the neighbours reply a Status message. On receiving the Status messages from the neighbours, the new node send Join to the leader node. After getting the Join message, the leader node adds the new node to its service list and divides its budget according to nodes reputation.

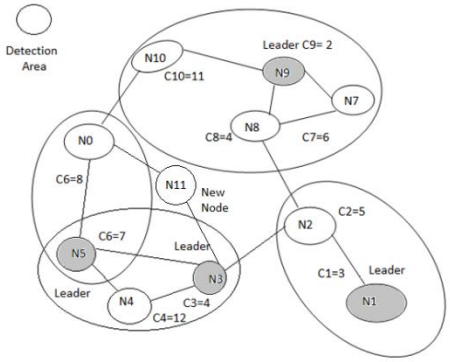


Fig 3.4 MANET after adding a new node

3.6.4 Removing a Node

When a node is disconnected from the network the neighbour nodes have to reconfigure the network. Whenever a node dies, its neighbours are aware of it. At first, a Dead (n) message is circulated to all neighbours to confirm the removal of node n. On receiving the Dead (n) message, the neighbour node k checks whether node n is its leader node or not. If node n is the leader node of node k, then node k announces a new election and updates its reputation table.

The Fig 3.5 given below depicts the removal of the node from the network.

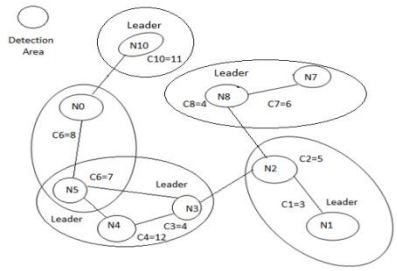


Fig 3.5 Removing a node

3.6.5 DISADVANTAGES OF EXISTING SYSTEM

- Not energy efficient.
- Network lifetime reduced by more energy consumption.

3.7 PROPOSED SYSTEM

Position-based routing protocols exhibit better scalability, performance and robustness against frequent topological changes. These routing protocols use the geographical location of nodes to make routing in networks. This will improve efficiency and performance of the network. The main aim of Position-based LAR1 is to reduce the control overheads by the use of location information.

LAR1 has two types of zone, Expected zone and Request zone, to restrict the flooding of route request packets. A source node uses the location service to find out the location of the destination and according to that information it will set the expected zone. Request zone is also determined by the source node and it is zone where a route request should be forwarded from source.

3.7.1 Expected Zone

Expected zone is set up by the source node S when it has data intended for destination node D. By using location service node S estimates the geographical location of node D at time t0. Suppose node D was at location O at time t_0, and that the current time is t_1. From this information node S is capable of determining the 'expected zone' of node D from the viewpoint of node S by time t_1. It is the region that node S expects to contain node D at time t_1.

For instance, if node D is travelling with average speed ν, then node S assumes that node D is in the expected zone of circular region of radius ν(t1 – t0), centered at location O. The expected zone is only an estimate made by node S to determine a region that may contain D at time t_1. Since, if actual speed of node D is greater than the average, then the destination D may actually be outside the expected zone at time t_1. Figure 1 shows the expected zone created by the source node S.

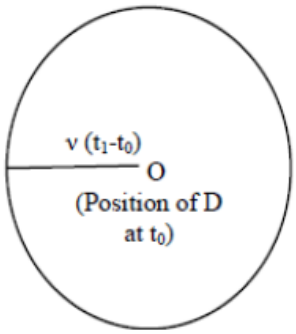


Fig 3.6 Expected Zone

3.7.2 Request Zone

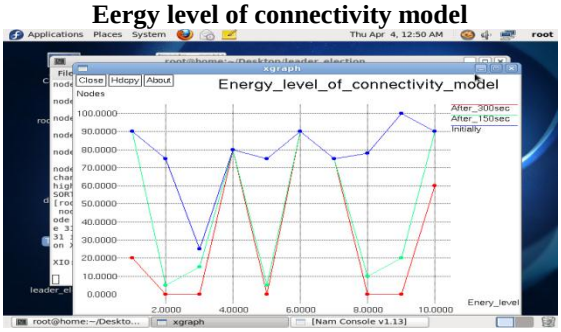
The 'request zone' is different from the expected zone. It is the zone where a route request should be forwarded from source. An intermediate node will forward a route request packet only, if it belongs to the request zone. The request zone should contain the expected zone to reach destination node D. The source node S defines this zone for flooding the route request packets. An intermediate node will forward the request packet, only if it is located within the request zone.

3.7.3 ADVANTAGES OF PROPOSED SYSTEM

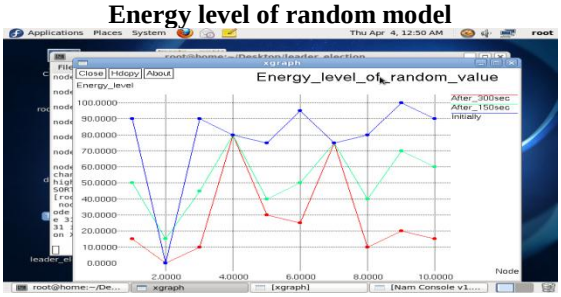
- Performance metrics such as packet delivery ratio, end to end delay, average energy consumption are efficient
- Overall energy consumption of the network is decreased by 20%.
-

3.7.4 OUTPUT:

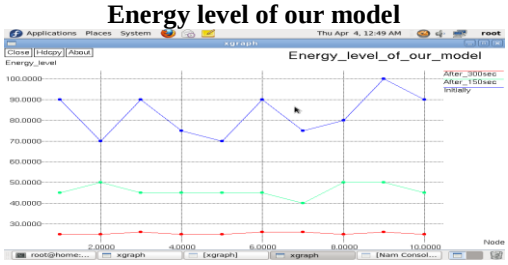
Eergy level of connectivity model



Energy level of random model



Energy level of our model



3.8 RESULT AND DISCUSSION

In this project the energy level of the connectivity model and random model and leader election with ELAR1-VAR protocol are compared.Theenrgy consumption by the random and connectivity model is high compared to the prosed technique.Hence the network life time is reduced in the connectivity and random model.But in the proposed technique smallest path is selected for transmitting the packet by using ELAR1-VAR protocol hence low energy is consumed and the network life time is increased.

REFERENCES

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

[2] L. Anderegg and S. Eidenbenz. Ad hoc-VCG: A truthful and costefficient routing protocol for mobile ad hoc networks with selfish agents. In proc. of the ACM International Conference on Mobile Computing and Networking (MobiCom), 2003.

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

[4] S. Basagni. Distributed and mobility-adaptive clustering for multimedia support in multi-hop wireless networks. In proc. of the IEEE International Vehicular Technology Conference (VTC), 1999.

[5] S. Basagni. Distributed clustering for ad hoc networks. In proc. of the IEEE International Symposium on Parallel Architectures, Algorithms, and Networks (ISPAN), 1999.

[6] M. Bechler, H. Hof, D. Kraft, F. Pahlke, and L. Wolf. A cluster based security architecture for ad hoc networks. In proc. of the IEEE INFOCOM, 2004.

[7] 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.

[8] 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.

[9] 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.

[10] B. DeCleene, L. Dondeti, S. Griffin, T. Hardjono, D. Kiwior, J. Kurose, D. Towsley, S. Vasudevan, and C. Zhang. Secure group communications for wireless networks. In proc. of the IEEE Military Communications Conference (MILCOM), 2001.

[11] J. Feigenbaum, C. Papadimitriou, R. Sami, and S. Shenker. A BGP based mechanism for lowest-cost routing. In proc. of the ACM symposium on Principles of distributed computing (PODC), 2002.

[12] J. Feigenbaum and S. Shenker. Distributed algorithmic mechanism design: Recent results and future directions. In proc. of the AMM International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIALM), 2002.

[13] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In proc. of the Cryptographic Hardware and Embedded Systems (CHES), 2004.

[14] S. Gwalani, K. Srinivasan, G. Vigna, E. M. Beding-Royer, and R. Kemmerer.An intrusion detection tool for AODV-based ad hoc wireless networks. In proc. of the IEEE Computer Security Applications Conference (CSAC), 2004.

[15] Y. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In proc. of the ACM International Conference on Mobile Computing and Networking (MOBICOM), 2002.

[16] 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.

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

[18] J.Green and J.Laffont. Incentives in Public Decision-Making. Springer Netherlands, USA, 1996.

[19] 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.

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

AUTHORS

First Author – Chitra.R, Student IV ECE, SNS College of Engineering, Coimbatore.
Second Author – Jayalakshmi.V, Student IV ECE, SNS College of Engineering, Coimbatore.
Third Author – Jayashree.R, , Student IV ECE, SNS College of Engineering, Coimbatore., E-mail id: jayraji.ece@gmail.com
Fourth Author – Keerthana.N, , Student IV ECE, SNS College of Engineering, Coimbatore.

Fifth Author – P.Karthik, Assistant Professor, SNS College of Engineering, Coimbatore.