The Cluster Leader Election in Manets

Mrs.P.Radhadevi*1, Sathish Ravula*2

Assistant Professor, Dept of Computer Applications, SNIST, Ghatkesar, Hyderabad, AP, India

M.C.A Student, Dept of Computer Applications, SNIST, Ghatkesar, Hyderabad, AP, India

ABSTACT:

A **mobile ad-hoc network** (**MANET**) is a self-configuring network of mobile routers connected by wireless links—the union of which form an arbitrary topology. When the size of the network grows, the amount of signaling overhead also increases to maintain the topology updates. One of the main issues of a MANET's routing protocol is hence its capacity to scale on large and dense networks. In this paper, we investigate the problems of cluster head selection for large and dense MANETs in the presence of selfish nodes for intrusion detection. One of the variants of cluster head selection Examined is: The size-constrained selection where each cluster is only allowed to have a limited number of members. To balance the resource consumption among all nodes and prolong the lifetime of an MANET, there are two main obstacles in achieving this goal: First, without incentives for serving others, a node might behave selfishly by lying about its remaining resources. Second, electing an optimal collection of leaders to minimize the overall resource consumption may incur a prohibitive performance overhead. To address the issue of selfish nodes, we present a solution based on mechanism design theory.

KEYWORDS: MANET, Leader election, intrusion detection systems, mechanism design.

I.INTRODUCTION:

Mobile Ad hoc Networks (MANETs) have no fixed chokepoints where Intrusion Detection Systems (IDSs) can be deployed [2]. Hence, a node may need to run its own IDS [1] and cooperate with others to ensure security [3], [4]. This is very inefficient in terms of resource consumption since mobile nodes are energy-limited. To overcome this problem, a common approach is to divide the MANET into a set of 1-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. The leader-IDS election process can be either random or based on the connectivity. Both approaches aim to reduce the overall resource consumption of IDSs in the network With both election schemes, 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 IDSs among nodes, this objective is difficult to achieve since the resource level is the private information of a node. Unless sufficient incentives are provided, nodes might misbehave by acting selfishly and lying about their resources level to not consume their resources for serving others while receiving others services.

When the size of the network grows, the amount of signaling overhead also increases to maintain the topology updates. One of the main issues of a MANET's routing protocol is hence its capacity to scale on large and dense networks. The two most popular techniques to reduce signaling overhead in MANETs are Fish Eye and clustering [7].In cluster-based routing, the network is divided into clusters. Each cluster has a cluster head (CH) node and some ordinary member nodes. MANET routing protocols are run in each cluster and their signaling messages are to propagate only within the cluster. The CHs notify each other about their cluster's members frequently using a different communication channel. Inter-cluster communications are relayed by CHs. The CHs may in turn form another MANET and be cauterized to an upper level if needed.

In order to reduce the overhead of the CH communications, the number of clusters must be minimized in the whole network. The CHs are thus spaced out to cover all nodes of the network and this also improves the spatial reuse of CH intra-communications. Therefore, most cluster-based techniques form non-overlapping clusters where CHs have multiple network interfaces with different communication ranges (*e.g.*: shortrange for intra-cluster and long-range for inter-cluster communications.) Notice that cluster-based technique can also be applied to MANETs where the nodes only have single network interface. In this situation, the inter-communication between distant CHs takes place as point-to-point communications.

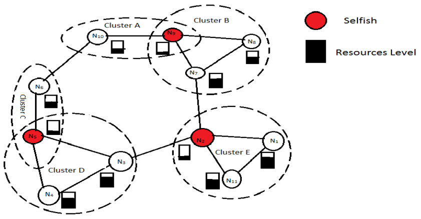

Fig.1. An example scenario of leader election in MANET

II.MOTIVATING EXAMPLE

Fig. 1 illustrates an MANET composed of 11 nodes labeled from N1 to N11. These nodes are located in five 1-hop clusters where nodes N5 and N9 belong to more than one cluster and have limited resources level. We assume that each node has different energy level, which is considered as private information. At this point, electing nodes N5 and N9 as leaders is clearly not desirable since losing them will cause a partition in the network and nodes will not be able to communicate with each other. However, with the random election model [3], nodes N5 and N9 will have equal probability, compared to others, in being elected as leaders. The nodes N5 and N9 will definitely be elected under the connectivity index-based approach due to their connectivity indexes finally, if the nodes N2, N5, and N9 are selfish and elected as leaders using the above models, they will refuse to run their IDS for serving others. The consequences of such a refusal will lead normal nodes to launch their IDS, and thus, die faster.

III. RELATED WORK

CH selection has extensively been studied in the literature of wireless ad hoc networks. It was showed in [5, 6] that using clusters for data-aggregation in large-scale sensor networks can significantly improve the sensors' lifetime. In [5], Heinzelman et al propose a protocol (LEACH) that allows nodes to select CHs using a distributed algorithm. Each sensor takes its turn as CH so that their energy consumption is balanced. LEACH ensures that the network has on average a fixed, predefined number of CHs at any time.

Chen et al [6] improve this approach by first estimating the optimal number of clusters to efficiently utilize data correlation of sensors. A new random CH selection algorithm is then proposed, aiming at minimizing the distance between the CHs and their members. Regarding MANETs, Chinara et al report in an interesting survey on clustering algorithms, They show that while nodes ID-based selection produces a fast and stable cluster setup, it suffers from the rigidness of the CHs' structure, because the same nodes are often selected independently of the network topology. We choose to consider the CH selection in this paper uniquely with the constraints related to the network topology graph, i.e. limiting the size of each cluster. The reason behind this limitation is because other metrics (e.g.: energy, traffic load, mobility factors) can often be modeled using an appropriate weighted graph topology.

IV.PROBLEM STATEMENT

We consider an MANET where each node has an IDS and a unique identity. To achieve the goal of electing the most cost-efficient nodes as leaders in the presence of selfish and malicious nodes, the following challenges arise: First, the resource level that reflects the cost of analysis is considered as private information. As a result, the nodes can reveal fake information about their resources if that could increase their own benefits. Second, the nodes might behave normally during the election but then deviate from normal behavior by not offering the IDS service to their voted nodes. 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_3,…, c_n} , where n is the number ofnodes 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. This will motivate the nodes to cooperate in every election round that will be held on every time T_{ELECT}. Thus, the model will be repeatable. For example, if B=25 packet/sec and the leader gets four votes, then the leader's sampling budget is 100 packet/sec. This value is divided among the four nodes based on their reputation value. The objective of minimizing the global cost of analysis while serving all the nodes can be expressed by the following Social Choice Function (SCF)

$$CSF = S(C) = min \sum_{k\in N} ck (\sum_{i\in N} vtk\,(C, i). B).$$

Clearly, in order to minimize this SCF, the following must be achieved. First, we need to design incentives for encouraging each node in revealing its true cost of analysis value c, which will be addressed in [3]. Second, we need to design an election algorithm that can provably minimize the above SCF while not incurring too much of the performance overhead.

V. LEADER ELECTION MECHANISM

In this section, we present our leader election mechanism for truthfully electing the leader nodes. To make the paper self-contained, we have four modules. They are: background on mechanism design, mechanism design model, cost of analysis function followed by the reputation system model.

VI. Mechanism Design Background

Mechanism design is a subfield of microeconomics and game theory. Mechanism design uses game theory [3] tools to achieve the desired goals. mechanism design allows a game designer to define rules in terms of the SCF such that players will play according to these rules. 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. The main goal of using mechanism design [3] is to address this problem by: 1) designing incentives for players (nodes) to provide truthful information about their preferences over different outcomes and 2) computing the optimal system-wide solution, which is defined according to SCF.

PS(Percentage of Sampling)	Class 1	Class 2	Class 3
After 200 sec	10%	15%	20%
After 500 sec	13%	18%	24%
After 800 sec	14%	20%	26%

VII. 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 qi. The type qi is drawn from each player's available type set Qi= {Normal, Selfish}. 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 Section 4, a detailed analysis is given. We assume that each player i has a utility function [3]: $u_i(q_i)=p_i-v_i(q_i,\circ(q_i,q_{-I}))$ where

- q_i is the type of all the other nodes except i.
- v_i is the valuation of player i of the output $\circ$ belongs $\circ$, knowing that $\circ$ is the set of possible outcomes. In our case, if the node is elected, then v_i is the cost of analysis ci. Otherwise, vi is 0 since the node will not be the leader, and hence, there will be no cost to run the IDS.
- pi belongs R is the payment given by the mechanism to the elected node. Payment is given in the form of reputation. Nodes that are not elected receive no payment.

VIII. 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 and should not be disclosed publicly. Such a disclosure of information can be used maliciously for attacking the node with the least resources level. 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 contribute and increase their reputation values. To solve the above problems, we design the cost of analysis function with the following two properties: Fairness and Privacy. The former is to allow nodes with initially less resources to contribute and serve as leaders in order to increase their reputation.

TABLE 1
PS Calculated by the Proposed Cost Function

Fig 2: Table 1

IX. Reputation System Model

Before we design the payment, we need to show how the payment in the form of reputation can be used to: 1) motivate nodes to behave normally and 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, we 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 our mechanism, a punishment system is needed to prevent nodes from behaving selfishly after the election. 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. Fig. 2 shows the abstract model of our reputation system where each node has the following components:

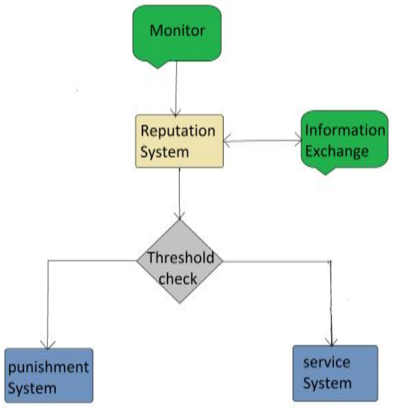

Fig3:Overall Architecture

Monitor or watchdog: It is used to monitor the behaviour of the elected leader. To reduce the overall resource consumption, we randomly elect a set of nodes, 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.

Information exchange: It includes two types of information sharing:- The exchange of reputation with other nodes in other clusters - To reduce the false positive rate, the checkers will exchange information about the behaviorof the leader to make decision about the leader's behavior.

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.

Threshold check: It has two main purposes:
- 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.
- To verify whether a leader's behavior exceeds a predefined misbehaving threshold. According to the result, the punishment system is called.

Service system: To motivate the nodes to participate in every election round, the amount of detection service provided to each node is based on the node's reputation. Each elected leader has a budget for sampling, and thus, only limited services can be offered. This budget is distributed among the nodes according to their reputation. Besides, this reputation can also be used for packet forwarding. Packets of highly reputed nodes should always be forwarded. On the other hand, if the source node has an unacceptably low reputation, then its packet will have less priority. Hence, in every round, nodes will try to increase their reputation by becoming the leader in order to increase their services.

Punishment system: To improve the performance and reduce the false positive rate of checkers in catching and punishing a misbehaving leader, we have formulated in [3] a cooperative game-theoretical model to efficiently catch and punish misbehaving leaders with low false positive rate. Our catch-and-punish model was made up of k detection levels, representing different levels of selfish behaviours of the leader-IDS. This enables us to better respond to the misbehaving leader-IDS depending on which detection level it belongs to. Hence, the percentage of checkers varies with respect to the detection level. Once the detection exceeds a predefined threshold, the leader will be punished by decreasing its reputation value.

X. Size-constrained CH Selection

There is a major drawback with the previous selection of a CH set. Because this mode of selection is based solely on the distance constraint, it offers no control over the size of each cluster. If some clusters are too large and the CHs have to relay a high amount of control traffic for their dependents then congestions may occur in the network. It can directly impact the network's quality of service. Figure shows the distribution of the cluster size for a network of *n* = 100 nodes with node density v=20.This distribution is obtained by averaging the simulation results of 20000 random network scenarios. The CHs are selected according to the distance-2 constraint, *i.e.* each node is either a CH or is within 2 hops from a CH. The *x* - axis depicts the size of clusters and the *y* -axis the percentage of nodes being in a cluster of that size. This percentage is calculated over 100 nodes and over 20000 random scenarios that we simulated. nodes (n)=100, density (πn/L2)=20, tries=20000

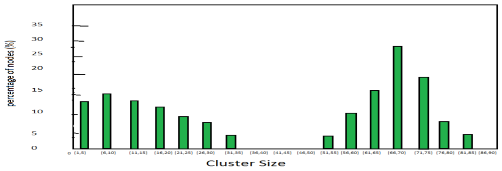

Fig4 : performance calculation

XI. CONCLUSION

The unbalanced resource 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. Moreover, the sum of the elected leaders is globally optimal. To achieve this goal, incentives are given in the form of reputations to motivate nodes in revealing truthfully their costs of analysis. Reputations are computed using the well-known VCG mechanism[3] by which truth telling is the dominant strategy.

Also according to our simulations, while the number of clusters in the network increases, the CH selection with size constraint can offer a more robust connectivity to the dependents. Its CH density is higher than 2 for most network configurations. That means if some CHs fail, their dependants may be able to find an existing CH in the neighborhood ready for a quick backup. Notice that this backup feature needs an additional protocol to help nodes recovering from a CH failure, which is a subject for further research.

XII. REFERENCES

[1] T. Anantvalee and J. W , “A Survey on Intrusion Detection inMobile Ad HocNetworks,” Wireless/Mobile Network Security, Springer, 2006.

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

[3] Noman Mohammed, “Mechanism design-based secure leader election model for intrusion detection in Manet”Proc. IEEE,2011.

[4] Dang Nguyen1, **“**On the Selection of Cluster Heads in MANETs” Proc. IEEE,2011.

[5] A. P. Chandrakasan, A. C. Smith, W. B. Heinzelman, and W. B. Heinzelman, “An application-specific protocol architecture for wireless microsensor networks,” IEEETransactions on Wireless Communications, vol. 1, no. 4, pp. 660–670, 2002.

[6] H. Chen and S. Megerian, “Cluster sizing and head selection for efficient data aggregation and routing in sensor networks,” in IEEE Wireless Communications and Networking Conference, WCNC 2006, vol. 4, April 2006, pp. 2318–2323.

[7] P. Brutch and C. Ko, “Challenges in Intrusion Detection forWireless Ad-Hoc Networks,” Proc. IEEE Symp. Applications and theInternet (SAINT) Workshop, 2003.