Progress in Nonlinear Dynamics and Chaos
Vol. 1, 2013, 65-70
ISSN: 2321 – 9238 (online)
Published on 11 November 2013
www.researchmathsci.org

Progress in
Nonlinear
Dynamics and Chaos

Mechanism Based Intrusion Detection for Balancing Resource Consumption in MANETs

***A. Reyana*[1] and *S. Priya*[2]**

[1] Department of Computer Science &Engineering,
Nehru Institute of Engineering and Technology, Coimbatore, India
Email: reyareshmy@gmail.com
[2] Department of Computer Science &Engineering
Nehru Institute of Engineering and Technology, Coimbatore, India
Email: riyapriya6@gmail.com

Received 13 September 2013; accepted 30 September 2013

Abstract. Here, the leader election in the presence of selfish nodes for intrusion detection in mobile ad hoc networks is given. There are two main obstacles in achieving this goal. First, without incentives for serving others. Second, electing an optimal collection of leaders to minimize the overall resource consumption. To address the issue of selfish nodes, a solution based on mechanism design theory is selected. To address the optimal election issue, a local election algorithm namely, Cluster-Dependent Leader Election (CDLE) is opted. Finally, the effectiveness of the proposed schemes is justified.

Keywords: Leader election, Mechanism Design, Intrusion Detection

1. Introduction

Unlike traditional networks, the Mobile Ad hoc Networks have no fixed chokepoints/ bottlenecks where Intrusion Detection Systems (IDSs) can be deployed. The nature of mobility for mobile networks needs additional mechanisms for providing security. These vulnerabilities do not exist in a fixed wired network. Therefore, the traditional way of protecting networks with firewalls and encryption software is no longer sufficient. Hence, a node may need to run its own IDS and cooperate with others to ensure security. This is very inefficient in terms of resource consumption since mobile nodes are energy-limited.

2. Survey Results

An initial approach to detect intrusions in ad hoc networks has been proposed in [5][6]. Reference [5] on the other hand considers specific mechanisms to detect a small set of attacks in wireless networks. The approach followed in [5] is to identify the misbehaving nodes by having limits on the information that should be given out by a node in a given period of time.

3. Module Description

The problem is divided into three modules:

A. Leader Election Mechanism: The leader election mechanism involves truthfully electing the leader nodes. The elected leader should be the most-valued-node from among all the nodes within that connected component, where the value of a node is a performance-related characteristic such as remaining battery life, minimum.

B. Cluster Dependent Leader Election: Cluster-Dependent Leader Election (CDLE) assumes the clusters of nodes and elects leaders after the network is formulated into multiple clusters. Here the leaders are elected in an optimal way in the sense that the resource consumption for serving as IDSs will be balanced among all nodes overtime. The algorithm decreases the percentage of leaders, single-node clusters, and maximum cluster size, and increases average cluster size.

C. Intrusion Detection System: An elected leader is responsible for detecting intrusions for a predefined period of time. The goal of this model is to detect selfish nodes and enforce them to cooperate. The dynamic and cooperative nature of the wireless ad-hoc network suggests that the intrusion detection system should be designed to be dynamic and cooperative as well.

4. System Implementation

4.1. Leader Election Mechanism

The leader election mechanism involves truthfully electing the leader nodes. Leader election is a fundamental control problem in both wired and wireless systems. When nodes are mobile, topologies can change and nodes may dynamically join/leave a network. In such networks, leader election can occur frequently, making it a particularly critical component of system operation. The classical statement of the leader election problem is to eventually elect a unique leader from a fixed set of nodes. Indeed, several algorithms have been proposed to solve this problem. However, in the context of mobile, ad hoc networks this statement must be specialized in two important ways, the election algorithm must tolerate arbitrary, concurrent topological changes and should eventually terminate electing a unique leader. The elected leader should be the most-valued-node from among all the nodes within that connected component, where the value of a node is a performance-related characteristic such as remaining battery life, minimum. The first modification is motivated by the need to accommodate frequent topology changes - changes that can occur during the leader election process itself. Existing solutions to the problem of leader election do not work in the highly dynamic environment found in mobile networks, as it assumes a static topology or assume that topological changes stop before an election starts.

4.1.1. Mechanism Design Model

The balance of IDS resource consumption problem can be modeled using mechanism design theory with a function that depends on the private information of the nodes. In this the private information of the node is the energy level, memory availability and node mobility. The mechanism model consists of two types of input: 1) the distance between the nodes and 2) the cluster range to which the node belongs to. According to the input given, each node selected in the path will reveal its resources in order to select the leader among them. The path contains any number of nodes that provides the shortest path to the destination. There may be many paths from source to destination. Therefore the selected path must reach the destination with minimum time and usage of minimum resources. The nodes that belong to a similar range are considered to be in the same cluster. Thus

based on the ranges the nodes are divided into multi clusters and there exist communication between the nodes of various clusters. The nodes are categorized into two types i.e. Selfish and Normal. The normal nodes follow the protocol, whereas selfish nodes deviate from the defined protocol if the deviation leads to a higher utility. Although the selfish nodes will not actively harm others but their presence can passively harm others.

4.2. Cluster Dependent Leader Election Algorithm

To address the optimal election issue, a series of local election algorithms is proposed, that can lead to globally optimal election results with a low cost. The issue is addressed by, Cluster-Dependent Leader Election (CDLE), this assumes given clusters of nodes and elects leaders after the network is formulated into multiple clusters. In this scheme, the leaders are elected in an optimal way in the sense that the resource consumption for serving as IDSs will be balanced among all nodes overtime. The algorithm decreases the percentage of leaders, single-node clusters, and maximum cluster size, and increases average cluster size. 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; and 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. Reputation-table (k): The reputation table of node k. Each node keeps the record of reputation of all other nodes. Neighbors (k): The set of node k's neighbors. Leader node (k): The ID of node k's leader. If node k is running its own IDS, then the variable contains k. Leader (k): A Boolean variable that sets to TRUE if node k is a leader and FALSE otherwise.

4.2.1. Algorithm

The formal algorithm is presented below.

Step1: Sends Hello Message
Step2: Choose Strategy :{Selfish, Normal}
If Selfish then
Sends False Information
Else
Election invoked
Step3: Number of Nodes n/Random number
Step4: For all n;
BV = {1 to 100}; // Charge in percentage
MA= {1 to 100}; // Memory Value
MR= {1 to 100}; //Mobility range
Step5: Update Neighbor node, Reputation table;
Step6: For all n Compare Charge, Memory availability and range
Step7: Election of leader
Step8: Sends Acknowledgement
Step9: Starts Intrusion Detection

4.2.2. Implementation of the Model

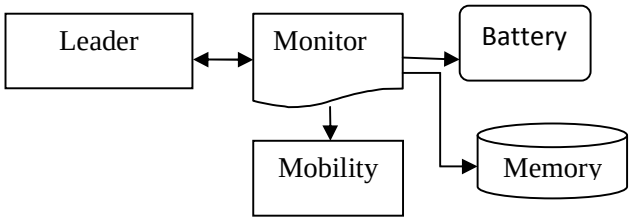

Figure 3.1. Mechanism Design Model

The cluster dependent leader election is conducted in order to choose the optimal and cost efficient leader. The leader node will have the list of nodes that participate in the network as neighbor nodes. This list is maintained in the table, Neighbour (k). The leader node is elected by monitoring the nodes that come into the network. If the nodes are of similar range then they are occupied in the same cluster. Each node in the network during leader election reveals their resource level, which is the private information of a node. The resource level considered here is the Energy level, Mobility and Memory availability. The energy level increases or decreases based on the services provided by the node. The node utilizes minimum energy in order to sustain itself in the network. Some nodes in order to save energy avoid itself in participating in elections. As the leader node has to provide services for others rather than itself. Mobility is that the node moves from one place to another for which its distance and cluster range varies. The memory availability may vary for each node based on the services and internal configuration. Since the mobile nodes are considered each time the node may move and need to adapt to other clusters. Thus here the selfish nodes are encouraged to participate honestly in leader election. Hence the node that is elected as leader will have maximum lifetime in the network. The leader election, the nodes are considered to be normal. The nodes can be normal or selfish based on their benefits. The normal nodes reveal only truthful information and they belong to a dominant strategy. Whereas the selfish nodes reveal untruthful information to avoid itself from being elected.

Node	Strategy	Battery	Memory	Mobility	Leader
N121	Normal	23%	16	3%	No
N626	Normal	2%	76	2%	No
N000	Normal	79%	98	57%	Yes

Table 1: Resource Calculation

In Table 1, there are three nodes in the network. The node names are chosen in random as N121, N626 and N000. The input for all the networks is the distance of the nodes and the range. For the node N121, N626, N000 the distance given is 10, 15, 17 and the ranges given 24, 19, and 28. Since the ranges here are similar the three nodes belong to one cluster. If there is a wide range of differences among the ranges then the nodes belong to several different clusters. In order to elect the leader the nodes in the network reveal their private information. Since the nodes are assumed to be normal the private

information is considered to be true. Thus comparing the three nodes the node N000 is elected as leader.

When the leader election gets over, the elected leader is responsible for transmission of packets in the network, protect all nodes in the network, and balance the resource consumption among all nodes in the network. Since the leader node has the list of all nodes in the network, this helps it to choose the shortest and secured path for packet transmission. Once the source and destination has been identified, the transmission route will be set. The model provides various paths from source to destination and opts the feasible path that provides reliable transmission. Since the path taken is the shortest it avoids collisions and transmission delays. As the packets are transmitted through the leader node, it also prevents security flaws like spoofing, cheating etc.

Node	Dist	Range	Strategy	Neighbor	Leader
N477	15	25	Selfish	-	No
N124	10	35	Normal	N477	No
N818	20	29	Normal	N477,N124	Yes
N427	22	40	Normal	N477,N81,N124	No

Table 2: Routing Path

Source Node N124 and Destination node N427. From Table 2, there exist different paths, they are as follows: N124->N818->N427, N124->N477, N427->N124, N477-N427, N818-> N427.Since the node N477 is selfish, no packets send through this route is forwarded. Hence the feasible and reliable path considered here is the N124->N818->N427.

4.3. Intrusion Detection

Due to the security needs in MANET, a cooperative intrusion detection model has been proposed, where every node participates in running its IDS in order to collect and identify possible intrusions. An elected leader is responsible for detecting intrusions for a predefined period of time. The goal of this model is to detect selfish nodes and enforce them to cooperate. Networks are protected using many firewalls and encryption software's. But many of them are not sufficient and effective. Therefore an intrusion detection system (IDS) is required that monitors the network, detects misbehavior or anomalies and notifies other nodes in the network. The ultimate goal of the security solutions for wireless networks is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users.

5. Conclusion

The unbalanced resource consumption of IDSs in MANET and the presence of selfish nodes have motivated 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. The result indicates that the normal nodes will carry out more duty of intrusion detection and die faster when there are more selfish nodes. Even though, the

algorithm used is able to prevent some security flaws such as spoofing, cache poisoning and avoid cheating. As selfish nodes do not exhaust energy to run the IDS service, it will live longer than the normal nodes. In the model, the node that has the least cost of analysis becomes the leader. In this way, all the nodes can keep a balance of their energy level with time. Hence, all the nodes will live long and die at the same time. As the number of nodes increases, the life of nodes also increases since there are more nodes to act as leaders. Thus, the detection service is distributed among the nodes which prolongs the live time of the nodes in MANET.

As an extension to the model, can include different sources of information such as routing and key distribution with different assigned weights. And can go for distributed leader-IDS election mechanism that can elect the most cost efficient leaders without running any clustering algorithm and analyzing traffic.

REFERENCES

1. N.Mohammed, H.Otrok, L.W.Debbabi and P.Bhattacharya, Mechanism design-based secure leader election model for intrusion detection in MANET, *IEEE Transactions on Dependable and Secure Computing,* 8(1) (2011) 89-103.
2. S.Madhavi and T.H.Kim, An intrusion detection system in mobile adhoc networks, *International Journal of Security and its Applications,* 2(3) (2008) 1-16.
3. V.Sivaranjani and D.Rajalakshmi, Secure cluster head election for intrusion detection in MANET, *Journal of Computer Application,* 5 (2012) 475-482.
4. L.Melit and N.Badache, An energy efficient leader election algorithm for mobile adhoc networks, *IEEE 2011,* C 978- 1- 4577- 0908- 1/11.
5. Rachedi and A. Benslimane, H. Otrok, N.Mohammed and M. Debbai, A mechanism design based secure architecture for mobile ad-hoc networks, *IEEE 2008 International Conference on Wireless and Mobile Computing, Networking and Communication* 978-0-7695-3393-3/ 08 DOI 10.1109.