Resource Constrained Leader Election Scheme for Intrusion Detection in Mobile Ad-Hoc Networks

K.Prabha[*], B.Kavi Priya[**], Dr.S.Sukumaran[***]

[*] Ph.D Research Scholar. Erode Arts and Science College, Erode-638009., Tamil Nadu, India.
[**] M.Phil Scholar, Erode Arts and Science College, Erode-638009., Tamil Nadu, India.
[***] Associate Professor of Computer Science, Erode Arts and Science College, Erode-638009., Tamil Nadu, India.

Abstract- Mobile Ad-hoc Network is a peer-to-peer wireless network that transmits data from computer to computer without the use of a central base station or access point. Intrusion detection techniques are used for the network attack detection process. The system is designed to handle leader election scheme for intrusion detection process. In this paper, we use leader election algorithm to find the globally optimal cost-efficient leader and it is devised to handle the election process for possibility of cheating and security flaws, such as replay attacks. The clustering scheme is optimized with coverage and traffic level. Cost and resource utilization is controlled under the clusters. The system development and analysis are carried out under the JiST (Java in Simulation Time) simulation environment.

Index Terms- Clustering, Leader Election, Detection Latency.

I. Introduction

A mobile ad-hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure[5]. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. Routing from one node to another node on mobile ad-hoc networks requires an "on-demand routing protocol," such as Dynamic Source Routing (DSR) or Adaptive On demand Distance Vector (AODV), which generates routing information only when a station initiates a transmission. The earliest mobile ad-hoc networks were called "packet radio" networks. In order to make our concept scalable, to avoid expensive long-range traffic, and to enhance availability by providing service locally, we partition an ad-hoc network into a number of clusters.

In each cluster, exactly one distinguished node, the Cluster Head (CH) is responsible for establishing and organizing the cluster. The CHs are responsible for sending CH beacons in their clusters, containing administrative information for the cluster members. Clustering is also used in some routing protocols for ad hoc networks. Routing is typically divided into two parts: Routing within a cluster (intra-cluster) and Routing between different clusters (inter-cluster). If a cluster-based routing protocol is used, the clusters established by the routing protocol can also be used for our security concept, and some additional advantages are to be expected.

1.1 Intrusion Detection

Intrusion Detection is one of key techniques behind protecting a network against intruders. An Intrusion Detection System is a system that tries to detect and alert on attempted intrusions into a system or network, where an intrusion is considered to be any unauthorized or unwanted activity on that system or network[15]. Extensive research has been done in this field and efficient IDS systems have been designed for wired networks. These systems usually monitor user, system and network-level activities continuously, and normally have a centralized decision-making entity.

Unlike traditional networks, the Mobile Ad-hoc Networks (MANETs) have no fixed chokepoints/bottlenecks where Intrusion Detection Systems can be deployed. 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. 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 to serve as the IDS for the entire cluster. The leader election process can be either random or based on the connectivity. Both approaches aim to reduce the overall resource consumption. 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.

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.

II. PROPOSED METHOD

The mobile ad-hoc networks are infrastructure less networks. The base station, routers and redirection switches are not used in the mobile ad-hoc network environment. Clustering techniques can be used to group up the mobile ad-hoc network nodes. The nodes are grouped with reference to the coverage values. The leader node is selected for the clusters.The energy level is considered in the leader node selection process.

The computational power and storage levels are also considered in the leader election process. The system is designed to handle leader election for intrusion detection process. The clustering scheme is optimized with coverage and traffic level. Cost and resource utilization is controlled under the clusters. Node mobility is managed by the system. The overall process is depicted in the following diagram:

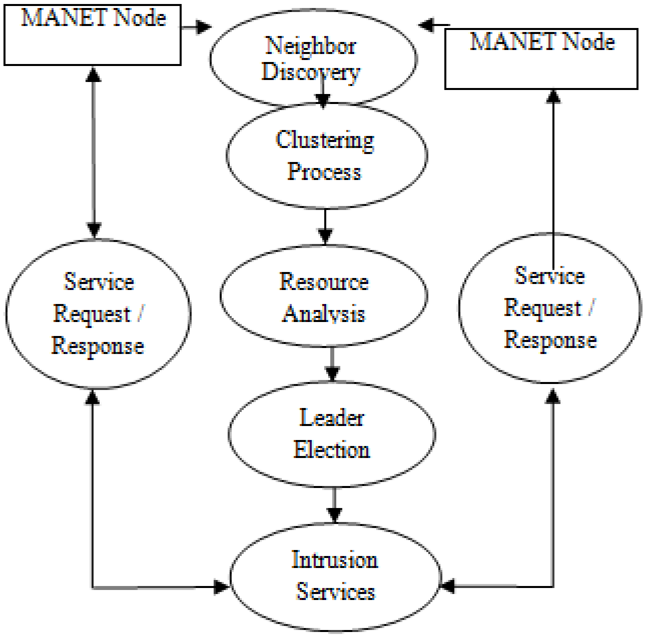


Fig 1. System Process

2.1 Leader Election Algorithm

To run the election mechanism, it is proposed that a leader election algorithm that helps to elect the most cost-efficient leaders with less performance overhead compared to the network flooding model. It devise all the needed the messages to establish the election mechanism taking into consideration cheating and presence of malicious nodes. The addition and removal of nodes to/from the network due to mobility reasons is considered. Finally, the performance overhead is considered during the design of the given algorithm where computation, communication, and storage overhead are derived.

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, the system uses the following notation:

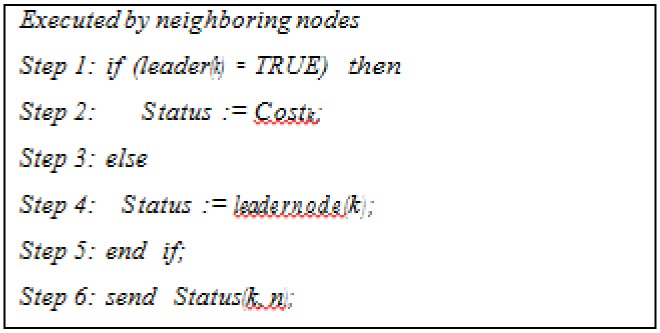
- Service-table (k): The list of all ordinary nodes, those voted for the leader node k.
- Reputation-table (k): The reputation table of node k. Each node keeps the record of reputation of all other nodes.
- Neighbors (k): The set of node k's neighbors.
- Leadernode (k): The ID of node k's leader. If 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.

Initially, each node k starts the election procedure by broadcasting a Hello message to all the nodes that are 1 hop from node k and starts a timer T_1. This message contains the hash value of the node's cost of analysis and its unique identifier (ID). This message is needed to avoid cheating where further analysis is conducted.

```
Executed by Elected leader node

Step 1: Leader(i) := TRUE;
Step 2: Compute Payment, $P_i$;
Step 3: update$_{service-table}$(i);
Step 4: update$_{reputation-table}$(i);
Step 5: Acknowledge = Pi + all the votes;
Step 6: Send Acknowledge (i);
```

```
Executed by every node
Step 1: if (received Hello from all neighbors) then
Step 2: Send Begin-Election ($ID_k$; $cost_k$);
Step 3: else if(neighbors(k) = $\phi$ ) then
Step 4: Launch IDS.
Step 5: end if
```



```
Executed by neighboring nodes
Step 1: if (leader(k) = TRUE) then
Step 2:     Status := $Cost_k$;
Step 3: else
Step 4:   Status := leadernode(k);
Step 5: end if;
Step 6: send Status(k, n);
```

III. RESULTS

The secure leader election system is tested under the simulation environment. The network transaction request data values are collected from University of California, Irwin (UCI) machine learning repository. The network transaction requests are initiated using the Defence and Research Project Agency (DARPA) data values. The benchmark data values are used in the intrusion detection process. All the intrusion detection operations are handled under the detector applications. The detector is assigned with reference to the cluster and resource information. The system uses two types of detector assignment methods. They are Cluster based Detector Assignment (CDA) and Cluster Integrated Detector Assignment methods (CIDA). In the cluster based model the detectors are assigned under the leader nodes of all clusters. In the cluster integrated model the detectors are assigned for a group up clusters. The detector count is reduced in the cluster integrated model. The energy consumption and traffic rate performance metrics are used to evaluate the system performance.

The energy consumption analysis is performed with different node count levels. The traffic rate analysis is performed to measure the bandwidth usage level for the mobile ad-hoc networks. The detection period for attack detection is measured in all detectors. The average detection period is measured as detection latency for the entire network.

3.1 Energy Consumption

A base station moderates communication among mobile nodes, scheduling and buffering traffic so that the mobiles can spend most of their time in the sleep state. In an ad hoc environment, there are no base stations and nodes cannot predict when they will receive traffic. Therefore, the default state in an ad hoc network is the idle state, rather than the sleep state.

Table 1.Energy consumption analysis between CDA& CIDA

Nodes	CDA(%)	CIDA(%)
20	81.3	69.8
40	84.6	72.1
60	87.4	75.6
80	91.3	79.2
100	94.8	81.4

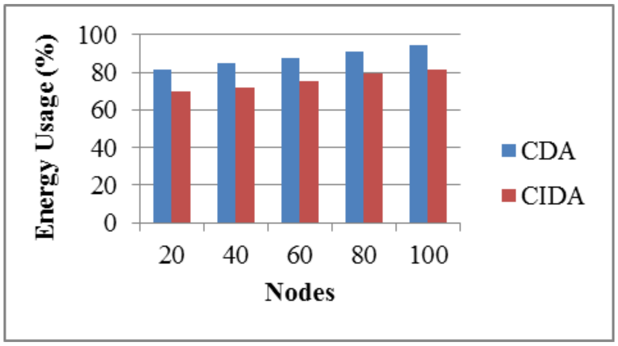


Fig 2. Energy consumption analysis between CDA & CIDA

The CIDA model reduces the energy consumption 10% more than CDA model.

3.2 Traffic Rate

The traffic rate analysis is used to evaluate the mobile ad-hoc network bandwidth usage levels. The bandwidth usage is estimated with reference to the number of packets transferred within the network environment. The traffic rate is the ratio between the number of packets transferred through the network and the number of packets transferred for the clustering operations.

Table 2. Rate analysis between CDA & CIDA

Nodes	CDA(%)	CIDA(%)
20	75.8	57.4
40	79.2	59.7
60	83.6	62.1
80	85.9	65.8
100	89.1	68.5

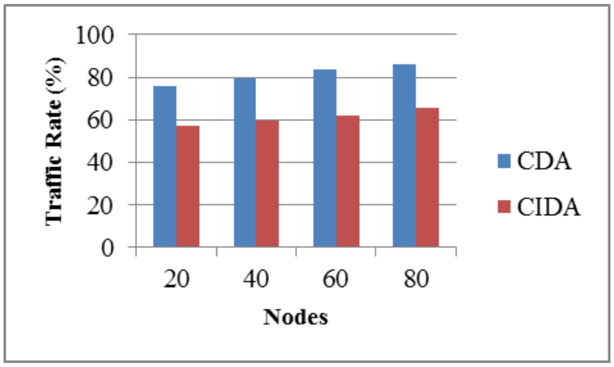


Fig 3. Rate analysis between CDA & CIDA

The CIDA model reduces the traffic rate 15% more than the CDA model.

3.3 Detection Latency

The detection latency analysis is used to measure the time taken for the intrusion detection process. The network request received time and request identification time difference is measured as delay period. The detection latency is the average time to detect the request type. The detection latency is measured in milli seconds.

Table 3. Detection Latency Analysis between CDA and CIDA

Nodes	CDA(%)	CIDA(%)
20	11.2	10.1
40	11.5	10.5
60	11.9	10.4
80	12.2	10.8
100	12.4	10.9

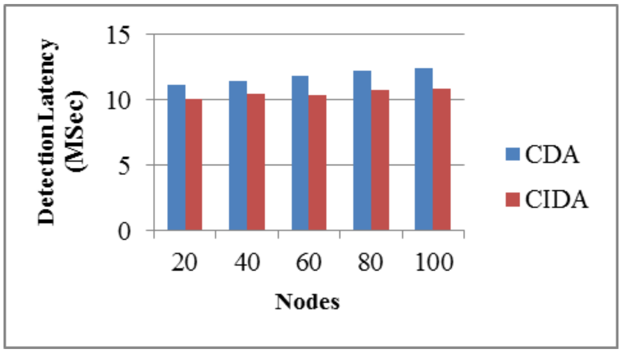


Fig 4. Detection Latency Analysis between CDA and CIDA

The CIDA model reduces the detection latency more than 15% then the CDA model. The detection latency is reduced in a considerable manner. The system reduces the energy consumption, traffic rate and detection latency measures.

IV. CONCLUSION

In this paper, we use a leader election algorithm to find the globally optimal cost-efficient leader. And it is devised to handle the election process for possibility of cheating and security flaws, such as replay attack. The clustering methods are used to group up the neighbor nodes. The CDA and Cluster CIDA models are used for the detector assignment process. The system reduces the energy consumption. Network traffic is reduced by the system. The system reduces detection latency in all network conditions. The leader election system can be adapted for the wireless mesh network environment. The intrusion detection system can be enhanced to manage key distribution process for data communication security. The signature based model can be integrated with the system to mprove the accuracy levels.

REFERENCES

[1] Arun K.Pujari, 'Data mining Techniques' University Press, First Edition, 2001.

[2] Azzedine Boukerche, 'Algorithms and Protocols for Wireless, Mobile Ad- Hoc Networks (Wiley Series on Parallel and Distributed Computing)', Publisher: Wiley - IEEE Press, 2008.

[3] M.Bechler, H.Hof, D.Kraft, F.Pahlke and L.Wolf, " A Cluster Based Security Architecture for Ad Hoc Networks," Proc. IEEE INFOCOM, 2004.

[4] K.Chen and K.Nahrstedt, "iPass: An Incentive Compatible Auction Scheme to Enable Packet Forwarding Service in MANET," Proc. Int'l Conf. Distributed Computing systems, 2004.

[5] Elliotte Rusty Harold, 'Java Network P rogramming', O'Reilly, 2nd Edition.

[6] S. Gwalani, K. Srinivasan, G. Vigna, E.M. Beding - Royer, and R. Kemmerer, "An Intrusion Detection Tool for ODV-Based Ad - Hoc Wireless Networks," Proc. IEEE Computer Security Applications Conf. (CSAC), 2004.

[7] Herbert Schildt, 'Java™ 2: The Complete Reference, Fifth Edition' McGraw-Hill, 2002.

[8] Y.Huang and W.Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2003.

[9] O.Kachirski and R.Guha, "Efficient Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," Proc. IEEE Hawaii Int'l Conf. System Sciences, 2003.

[10] Kegen Yu and Eryk Dutkiewicz, "Geometry and Motion- Based Positioning Algorithms for Mobile Tracking in NLOS Environments", IEEE Transactions on Mobile Computing, Vol. 11, no. 2, February 2012.

[11] Mohammad lyas, 'The Handbook of Adhoc Wireless Networks' CRC, 2002.

[12] N . Mohammed, H . Otrok, L. Wang, M .Debbabi, and P.Bhattacharya, "A Mechanism Design-Based Multi-Leader Election Scheme for Intrusion Detection in Manet," Proc. IEEE Wireless Comunication and Networking Conf. (WCNC), 2008.

[13] 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. 8, No. 1, January-February 2011.

[14] H. Otrok, N. Mohammed, L. Wang M. Debbabi, and P.Bhattacharya, "A Game - Theoretic Intrusion Detection Model for Mobile Ad-Hoc Networks," J. Computer Comm., vol. 31, no. 4, pp. 708-721, 2008.

[15] Sudip Misra, Isaac Woungang and Subhas Chandra Misra 'Guide to Wireless Ad Hoc Networks (Computer Communications and Networks)', Publisher: Springer, 2009.

[16] K.Sun, P.Peng, P.Ning, and C.Wang, "Secure Distributed Cluster Formation in Wireless Sensor Networks," Proc. IEEE Computer Security Applications Conf. (ACSAC), 2006.

[17] Y.Thomas Hou, Yi Shi, Jia Liu , Sushant Sharma, Sastry Kompella and Scott F. Midkiff, "Network Coding in Cooperative Communications: Friend or Foe?", IEEE Transactions on Mobile Computing, vol. 11, no. 7, July 2012.

[18] S.Vasudevan, B.DeCleene, N.Immerman, J.Kurose, and D.Towsley, "Leader Election Algorithms for Wireless Ad Hoc Networks," Proc. IEEE DARPA Information Survivability Conf. and Exposition (DISCEX III), 2003.

[19] Y.S.Vasudevan, B.DeCleene, N.Immerman, J. Kurose, and D. Towsley, "Leader Election Algorithms for Wireless Ad Hoc Networks," Proc. IEEE DARPA Information Survivability Conf. and Exposition (DISCEX III), 2003.

[20] Wenbo Mao "Modern IDS : Theory and Practice" Publisher: Prentice Hall PTR; 1st edition 2003.

AUTHORS

First Author – K.Prabha, Ph.D Research Scholar. Erode Arts and Science College, Erode-638009., Tamil Nadu, India.
Second Author – B.Kavi Priya, M.Phil Scholar, Erode Arts and Science College, Erode-638009., Tamil Nadu, India.
Third Author – Dr.S.Sukumaran, Associate Professor of Computer Science, Erode Arts and Science College, Erode-638009., Tamil Nadu, India.