International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 11, November 2014 **ISSN 2319 - 4847**

An Artificial Intelligence Based Multi-Leader Election Scheme for Eliminating Intrusion and Routing Attack in MANET

Dipashree Panda[1], Nirjharinee Parida[1] and Narendra Kumar Rout[2]

[1] Department of electronics and engineering, ITER, SOA University,Odisha

[1] Department of Computer science, SIET ,Dhenkanal, BPUT, Odisha

[2]Department of Computer Science, GEC, Bhubaneswar,BPUT, Odisha

ABSTRACT

A mobile ad-hoc network (MANET) is an independent system of mobile stations connected by wireless connection of network. Mobile host does not guarantee any fixed infrastructure and with the advance in technology for network crime is new threat to the centralized network management. Thus leader among the network node is having maximum risk. This paper proposed an artificial intelligence based model for multiple leader election and proposed intrusion detection algorithm in MANET. This paper propose a scheme for electing cluster leaders that have two advantages: First, the collection of elected leaders is the optimal in the sense that the overall resource consumption will be balanced among all nodes in the network overtime. Second, the scheme provides the leaders to detect intrusion or routing attack and take necessary action. Simulation shows that our model effectively prolongs the overall lifetime of IDS in MANET and balances the resource consumptions among all the nodes.

Keywords: MANET, intrusion detection, routing attack, leader election, network crime.

1. INTRODUCTION

MANET is an independent system of mobile stations connected by wireless connection to form a network. The cooperation among nodes is a crucial requirement for intrusion detection in Mobile Ad hoc Networks (MANETs) due to the autonomous nature of such networks [1-2]. In particular, a common approach for reducing the overall resource consumption of intrusion detection in MANET is for nodes to collaborate in electing a leader to serve as the intrusion detection system (IDS) for a cluster of one hop nodes. The election process can be either random [3] or connectivity [4] based. Both approaches aim to reduce the overall resource consumption of IDSs in the network. However, it is notice that nodes may have different remaining resources at any given time and this should be taken into account by an election scheme. 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 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. Figure1. Illustrates a MANET composed of eight nodes named as {A, B, C, D, E, F, G, F}. These nodes are located in two clusters composed of two- hop nodes that can overhear each other (node C and F belongs to both clusters). Suppose node 'C' currently has the least remaining resources , and 'B' and 'H' both belongs to different cluster wants to communicate through 'C'.

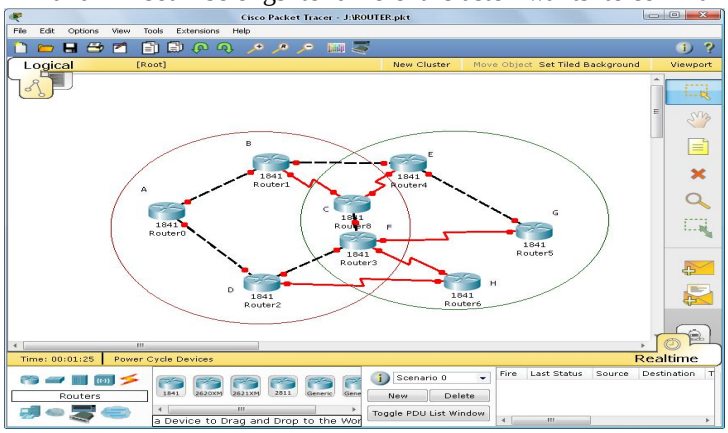


Figure1. Leader Election in MANET

At this point, electing node 'C' as a leader is clearly not desirable since losing 'C' will increase the cost of communication as new path can be B-E-G-F-H or B-A-D-H or B-A-D-F-H. However, with the random election model [3], node 'C' will have equal probability in being elected as a leader, whereas node 'C' and 'F' will definitely be elected under the connectivity index-based approach since they are connected to all nodes in both clusters [8]. Moreover, if both 'B' and 'H' are faulty and elected as leaders by the above models, then they will refuse to run their IDS for serving others. The consequences of such a refusal will lead normal nodes to lunch their IDS and thus die faster than others. This paper proposed an artificial intelligence based model for multiple leader election and proposed intrusion detection algorithm in MANET. More specifically, we design a scheme for electing cluster leaders that have the following advantages: First, the collection of elected leaders is the optimal in the sense that the overall resource consumption will be balanced among all nodes in the network overtime. Second, the scheme provides the leaders to detect intrusion or routing attack and take necessary action. Simulation shows that our model effectively prolongs the overall lifetime of IDS in MANET and balances the resource consumptions among all the nodes. The rest of this paper is organized as follows: Section II reviews related work. Section III Proposed Model. Section IV election scheme. Section V presents simulated results. Finally, Section VI concludes the paper

2. RELATED WORK

Various IDS techniques have been proposed in the research literature. Amandeep Makkar etal [5] and sunil tenaja etal [6] has described behavior study of MANET routing protocol such as optimized link state routing (OLSR), destination sequenced distance vector (DSDV), dynamic source routing (DSR), adhoc on-demand distance vector (AODV) and temporary ordered routing protocol (TORA) protocols, have been carried out so as to identify which protocol is most suitable for efficient routing over Mobile Adhoc NETwork (MANET). Nitiket N Mhala etal [7] describe an approach for determining conditions for monitoring of critical nodes for MANET intrusion detection system, he used trigger mechanism for the invocation of critical node test for MANET intrusion detection system. N. Vimala etal [8] in his work suggested efficient group key management protocol for region based MANETs, this method is also effective in defending against many sophisticated attacks such as denial of service (DoS) attack. A.Rajaram etal [9] describes power aware routing for MANET using on-demand multipath routing protocol, power aware adhoc on- demand multipath distance vector (PAAOMDV) is proposed to overcome the issue of energy and shortest path in a single routing protocol. This protocol helps in updating the routing table with both the node route list and their corresponding energies. Noman Mohammed etal [10] proposed a mechanism design based multi leader election scheme for intrusion detection in MANET, his work proposed a scheme for electing cluster leaders that have the two advantages: First, the collection of elected leaders used to balance the resource consumption. Second, the scheme provides the leaders with incentives in the form of reputation so that nodes are encouraged to honestly participate in the election process. Maha Abdelhaq etal [11] proposed a method for detecting resource consumption attack over MANET using an artificial immune algorithm, objective is to utilize the biological model used in the dendritic cell algorithm (DCA) to introduce a dendritic cell inspired intrusion detection algorithm (DCIIDA). DCIIDA is introduced to detect the resource consumption attack (RCA) over MANET.

3. PROPOSED WORK

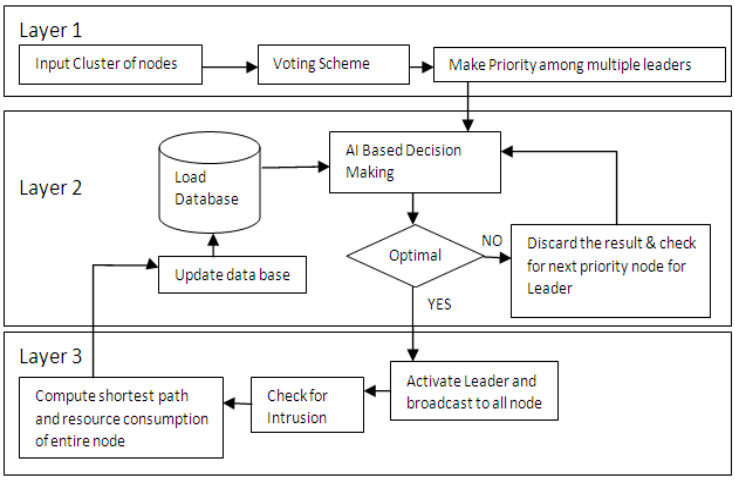


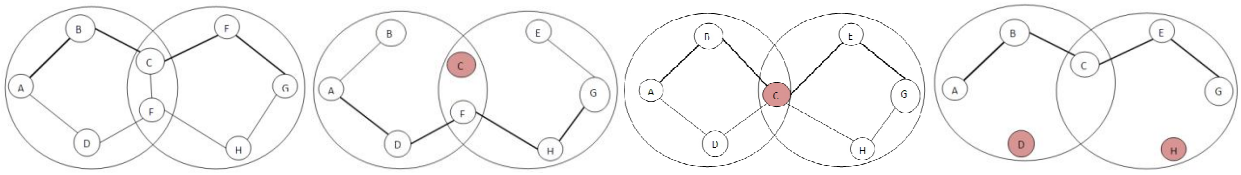
Figure2. Proposed Model

In particular, a common approach for reducing the overall resource consumption of intrusion detection in MANET is for nodes to collaborate in electing a leader to serve as the intrusion detection system (IDS) for a cluster of multi hop nodes. The election process can be either random or connectivity based. Both approaches aim to reduce the overall

resource consumption of IDSs in the network. We have proposed a three layer system for leader election as shown in figure 2. Layer 1 helps in finding leader and rank those leader according to their resource consumption. We call layer 1 as Election layer. Layer 2 is heart of the model. It accept leader in priority order from layer 1. It checks the effect of node to become leader on network, resource consumption, power, message broadcast time etc. If it find it as a optimal leader then elect it as leader, else check for the next node. We call layer 2 as Decision layer. In layer 3 the leader broadcast its ID to the entire node. New leader check for any intrusion or attack in the network then compute the shortest path among entire node of its cluster. Finally the database is updated with information of having new ID as leader, shortest path and resource consumption among entire node.

4. ELECTION SCHEME

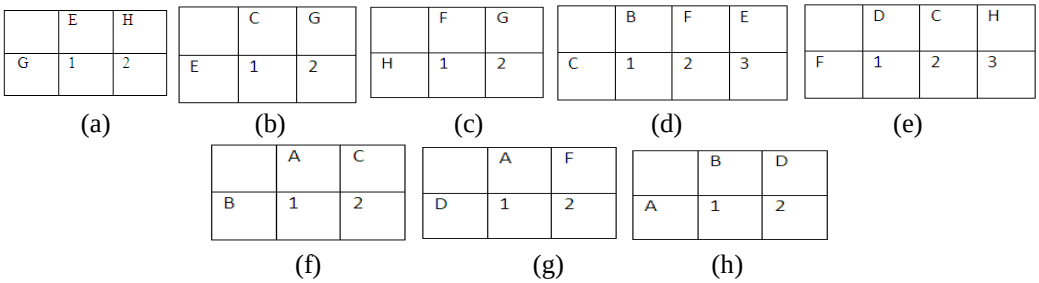
Voting scheme can be random or collaborative. Let us assume a network shown in figure 1. The node {A, B, C, D, E, F, G, H}is placed in two cluster C1 and C2. Each cluster know there leader and shortest path among each node. Let us assume the shortest path for the communication between A to G is shown in figure 3(a) as A-B-C-F-G in bold line. Surely at this point if C is elected as a leader then it refuses to serve the communication between A to G. At this point network deals check for the other best suitable path for the communication and can make the communication through A-D-F-H-G as shown in figure 3(b), and Node C does not serve other, and act as leader for both clusters. Now consider the figure 3(c), where election of node 'C' can cause the isolation of two clusters. Hence C cannot be made leader. Now for next alternate we are left with node A-B-D for C1 and G-F-H for C2 to take part in election. As A, B, F, G is actively taking part in communication hence we left with only two node D and H as a leader for cluster C1 and C2 respectively shown in figure 3(d).



(a) (b) (c) (d)

Figure3. (a) path ABCFG is used for communication between A to G (b) Leader Election – node C denies service and ADFHG is selected as new path for communication between A to G. (c) Leader Election – node C cannot be made leader as it will break the cluster into two part, as it is the only node for communication (d) node D and H is chosen as leader for cluster.

Each node have buffer and information about the shortest path. So each node is treated as a vector of length equal to number of node in cluster. Initially all the vector is initialized to zero. Consider the figure 3(a), Let A wants to communicate with G, it sends the signal to its neighbour {B, D} for find shortest distance to G. Then {B, D} sends the same signal to C and F respectively. Now C and F send the signal to their neighbour. After some time signal reaches to G from different path say P= {A-B-C-E-G, A-D-F-H-G, A-D-F-C-E-G, A-B-C-F-H-G} in first come basis. As A-B-C-E-G reaches to G first hence it gives it as first priority. Then A-D-F-H-G is given second priority and so on. This priority table and path matrix P is broadcasted to all node. Now the buffer information of node A which was initialized with zero is now initialized with new priority information and path matrix p as shown in figure 4. Each node keeps track of its neighbour. Looking to P(1)=A-B-C-E-G and P(2)=A-D-F-H-G, G receives signal from E first then H, for which node G update its Buffer as shown in Figure 4(a) which depicts that the shortest path for G to communicate from A is through node E, then node H. Figure 4(b) depicts that shortest path for E to communicate from A is through node C then G. similarly figure 4(d) depicts that shortest path for C to communicate from A is through node B then F or E. figure4(f) depicts that shortest path for B to communicate through A is A then C. Hence we get a path ABCEG as a path communication.



(a) (b) (c) (d) (e)

(f) (g) (h)

Figure 4. (a) Buffer at G: E is closer to G then H (b) Buffer at E: C is closer to E then G (c) Buffer at H: F is closer then G (d) Buffer at C: B is closer to C then F and E (e) Buffer at F: D is closer to F then C and H (f) Buffer at B: A is closer then C (g) Buffer at D: A is closer to D then F. (h) Buffer at A: B is closer then D

Case1. Consider node C elected as leader in figure 3(a). By doing so the figure 4(d) is initialized to zero because node C refuses to serve other. As node C was using node B as first priority, but after election this line is no more providing service, therefore node B has to choose his alternate option. Now in figure 4(f), node B is closer to A, that means it direct take input from source i.e., node A, hence it report no path ahead for communication through B. Now node A has to search its other neighbour that is D whether he can establish the network or not. Looking to figure 4(g) node D can accept data from A. then figure 4(e), node F can accept data from node D, figure 4(c), node H can accept data from F and figure 4(a), node G can accept data from A. New path is constructed as A-D-F-H-G for communication as shown in figure 3(b).

Case2. Consider node C elected as Leader in figure 3c. New Buffer matrix will look like figure 5.

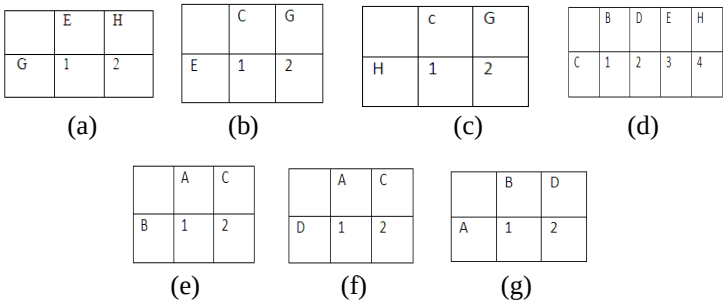


Figure5. (a) Buffer at G: E is closer to G than H (b) Buffer at E: C is closer to E than G (c) Buffer at H: C is closer than G (d) Buffer at C: B is closer to C than D, E, H (e) Buffer at B: A is closer than C (f) Buffer at D: A is closer to D than C. (g) Buffer at A: B is closer than D.

As C is selected as leader will result in kill of link to node B, D, E, and H. Looking figure 5(e), A is direct node connected to B. Hence A has to search for next path. Figure 5(f). Node D can be used for communication but node D links again with node C for communication in figure 5(d). Therefore node D cannot be selected. Now node A doesn't have any other neighbour, Hence the network management doesn't allow node C to be elected as leader, as it breaks the communication.

Case3. Who can be leader if node C can not be leader: From the figure 5, checks for those figure which do not have node C. we will find figure 5(a) and 5(g) are such node. Then check for the path through which communication is going on. i.e., A-B-C-E-G. Now figure 5a and 5g is combined to give us node {G, E, H, A, B, D}, subtract this with the path P.

$$\{G, E, H, A, B, D\} - \{A, B, C, E, G\} = \{H, D\}$$

Now node H and node D can be used for leader or can participate in election as shown in figure 4(d).

Case4. In the figure 6 node X could report the node Y is not forwarding packets in fact it does. This will cause S (Source) to mark Y as misbehaving when X is the real culprit.

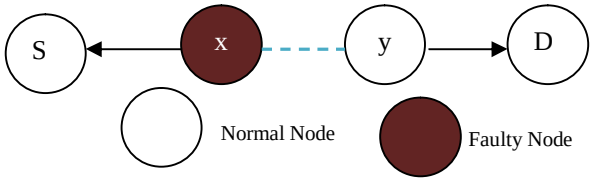


Figure 6. Faulty node x, gives false inspiration of Y as misbehave

Our method deals with the issue by maintaining the buffer and some timer for message transcription. Consider the figure 4(a). Suppose node B is a fault node and report that node C is not forwarding the packet. Now node C is isolated from the network by which new path become A-D-F-H-G. But as we know B is faulty, that means we should catch B not C. So we have designed a protocol named as wait and watch. In case of any misbehave done by any node, network wait for verification. After watching the verification result only decision is taken. After the report of node B that node C is misbehaving, Node A search for next option to send data which can go through node C but not through node B from path P= {A-B-C-E-G, A-D-F-H-G, A-D-F-C-E-G, A-B-C-F-H-G}. We get a path A-D-F-C-E-G. Now source A sends a packet through this path and wait for acknowledgment. If it get acknowledgement then it report node B as misbehaving node, now node B is isolated from network. Next best path apart from node B is then taken with the procedure discussed in case1. Here node B will be punished and new path will be found out.

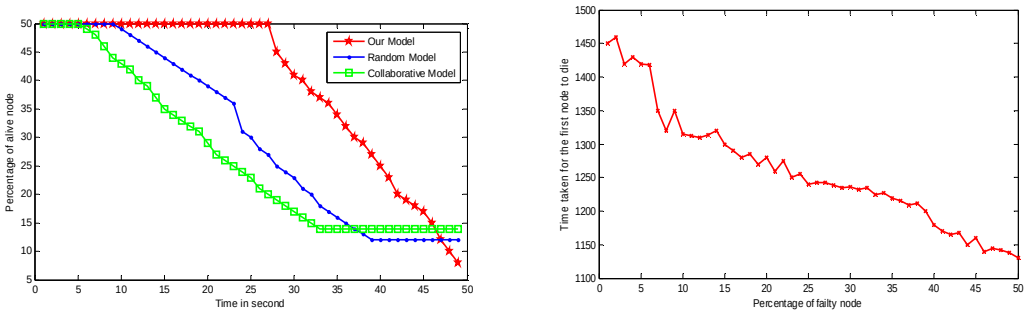
Algorithm 1 (Executed by every node for start Election – initiated from layer 1)
msg= message from the neighbor for election after each time T PriorityIndex is the set of shortest path from node to its neighbor Function startElection(msg, T) if (msg && T) update (ID,resources,PriorityIndex) endsend(ID,resource,PriorityIndex) end

Algorithm 2 (Executed by control system of layer 2 with Artificial Intelligence capacity)
/*PriorityIndex of elected node as leader is checked for optimality*/
Function decisionMaking(ID, Resource, PriorityIndex)
Read dataBuffer
Set leaderElected=0;
do
if isOptimal(Node) && qualify all cases
set leaderElected=1;
Launch ID as leader
else
check for next priorityIndex
end
while(leaderElected)
end

Algorithm 3 (Executed by Elected leader node of layer 3)
// Send Acknowledge message to the neighbor nodes
Function LeaderWork()
leader(i) := true;
Check for intrusion and shortest path
update - database
Acknowledge = Pi + all the votes;
Send Acknowledge(i);
Launch IDS.
end

5. SIMULATED RESULT

Our simulation was carried out with 50 numbers of nodes out of which 15% nodes were faulty. Figure 7(a), Depicts the percentage of live nodes as compared with other two models. To show the seriousness of misbehave, Figure 7(b) depicts behaviour and impact of faulty nodes on first normal node life. Result clearly indicates that normal nodes will overloaded with more work for intrusion detection and will die faster. Every 'T' time's nodes repetitively elect a set of leaders. The election is based on our proposed scheme. The result clearly prevails that our model provides higher percentage of alive nodes, in response to other models. Whereas random model elects leader without considering the energy level and make nodes with low energy to die faster. The connectivity index-based model elects leaders based on their peer connections. In most of the cases such as static scheme or mobility scheme, the model elects the same node repeatedly, due to which normal nodes die faster even when there is no faulty nodes.



(a) (b)

Figure 7. (a) Percentage of alive node (b) Time for the first node to die

6. CONCLUSION

MANETs is a wide area of research not only in civil communication but in defence also. We have used wait and watch method for finding faulty node and used better buffer based path finding technique for shortest path. Our distributed

mechanism was able to elect the most cost-efficient nodes. Simulation results showed that our model is able to prolong the lifetime of the network and balance the overall resource consumptions among all nodes.

References

[1] Y. Hu and A. Perrig. "A survey of secure wireless ad hoc
[2] routing", IEEE Security and Privacy, pp.28–39, 2004.
[3] A. Mishra, K. Nadkarni, and A. Patcha. "Intrusion detection in wireless ad hoc networks" . IEEE Wireless Communications, pages 48–60, 2004.
[4] Y. Huang and W. Lee." A cooperative intrusion detection system for ad hoc networks" . In Proceedings of the 1st ACM Workshop Security of Ad Hoc and Sensor Networks, pages 135–147, Virginia, ACM. , 2003
[5] O. Kachirski and R. Guha. " Effective intrusion detection using multiple sensors in wireless ad hoc networks" . In 36th Annual Hawaii International Conference on System Sciences, Jan. 2003.
[6] Amandeep Makkar, Bharat Bhushan, Shelja, and Sunil Taneja,"Behavioral Study of MANET Routing Protocols", International Journal of Innovation, Management and Technology, Vol. 2, No. 3, June 2011
[7] Sunil Taneja, "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, ISSN: 2010-0248, August 2010
[8] Nitiket N Mhala1 and N K Choudhari , " An Approach for Determining Conditions for Monitoring of Critical Nodes for MANET Intrusion Detection System", International Journal of Future Generation Communication and Networking Vol. 4, No. 1, March 2011
[9] N. Vimala B. Jayaram Dr. R. Balasubramanian, "Efficient Group Key Management Protocol for Region Based MANETs", IACSIT International Journal of Engineering and Technology, Vol.3, No.1, ISSN: 1793-8236, February 2011
[10] Dr.A.Rajaram and J.Sugesh ," Power Aware Routing for MANET Using On-demand Multipath Routing Protocol ' , IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, ISSN(Online): 1694-0814, July 2011
[11] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya," A Mechanism Design-Based Multi-Leader Election Scheme for Intrusion Detection in MANET", IEEE, WCNC, 2008
[12] Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail and Daud Israf, "Detecting Resource Consumption Attack over MANET using an Artificial Immune Algorithm", Research Journal of Applied Sciences, Engineering and Technology 3(9): 1026-1033, ISSN: 2040-7467, 2011

AUTHOR

Dipashree Panda have completed her B.tech (Electronics and Tellecommunications) in 2009 from krupajal engineering college under BPUT . She completed her M.Tech on VLSI and Embedded system in 2012 from ITER college under SOA University. She have worked as asst. Prof. at Mahavir engg college. Her area of interest is Ad-hoc network and VLSI

Nirjharinee Parida have completed her B.tch and M.tech from BPUT university in 2003 and 2013 respectively. Since 2005 she has been working as Ass. Prof in Synergy Institute of Engineering and Technology, Dhenakanal , BPUT ,Odisha. Her area of interest is Ad-hoc network and software engineering.

2Narendra Kumar Rout received the B.Tech.. Degrees in Computer Science and Engineering from BPUT , ODISHA and M.Tech. College of Engineering and Technology, Bhubaneswar, BPUT, Odisha in 2005 and in 2012 respectively, He is an author of many national and international Journals. His areas of research are artificial intelligence, swarm optimization and ad-hoc networks. He is a life member of Indian Society of Technical Education ,Computer Society of India and IEEE student member.