IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013
ISSN: 2320 - 8791
www.ijreat.org

Anomaly Intrusion Detection in MANET Using Dynamic Agent

C.Baskaran[1], S.Alangaram[2], M.Karuppasamy[3]

[1]Assistant Professor, Sudharsan Engineering College, Tamilnadu.
[2]Assistant Professor, Jaya Engineering College, Tamilnadu.
[3]Assistant Professor, Sri Nandhanam College of Engg &Tech, Tamilnadu.

ABSTRACT

Wireless ad hoc networks vulnerable to intrusions as they operate in an open medium and use co-operative strategies for the network communications. The solutions that are designed for wired networks are not always suitable for wireless networks, especially Mobile Ad Hoc Networks (MANET) Dynamic nature. To obtain a suitable level of security for MANET's, established security solutions like Agent (mobile agent) based are combined with intrusion detection mechanisms. One method is to have IDS client is running on every mobile host in a network, which runs a local uncovering engine analyzing local data for anomaly. A cooperative detection mechanism decides whether there is an intrusion occurs, with all nodes taking part in the decision process related negotiator (mobile agent). But MANET nodes typically limited battery power backup only. Thus it is not efficient to make each MANET node always a monitoring node. Instead a cluster of nearby MANET nodes can randomly and fairly elect a monitoring node use agent and the cluster head. Once a compromised node happens to be selected as the cluster head, it can begin attacks without being detected.

Index Terms- mobile ad hoc network (MANET), cluster head, mobile agent, and fitness function.

I. INTRODUCTION

INCEASINGLY, mobile ad hoc networks(MANETs) are receiving more attention as part of next generation network technologies. MANET is usually constructed by using mobile and wireless hosts with minimum or no central control point of attachment, such as a base station. These networks can be useful in a variety of applications, such as one off meting networks, disaster and military applications, and the entertainment industry. Because the network topology of MANETs frequently changes, and there is no central management entity, all of the routing operation must be performed by individual nodes in a collaborative fashion. Consequently, it is unrealistic to introduce an authentication server that can employ conventional cryptographic schemes to secure the network against attacks from malicious hosts. The typical types of attacks in MANETs include eavesdropping, address spoofing, forget packets, denial of service (dos), etc.

The cluster network organization contains many clusters with one cluster head node for each cluster. The cluster head are vested with additional responsibilities of coordinating, monitoring, allocating resources to its members; inter cluster and intra cluster communication among the nodes in the network [11]. The set of cluster head is known as the dominant set. A dominant set is a subset of nodes in the network that assures that every node is either in the subset or a neighbor of node in the subset [2]. Due to mobility nature of mobile nodes, frequent change in cluster head occurs that perturbs the stability of the network and affecting other protocols that rely on it and incurring high computation overhead caused due to information exchange among the nodes. Therefore it is desirable to choose the optimum number of the cluster head in the network. Every member of a population is associated with the certain fitness value that represents the degree of correctness or quality of solution. The genetic algorithm is used to optimize many clustering protocols.

To select cluster head based on this factor those are bandwidth of cluster, cluster ratio, battery power consumption of cluster head.

II. BACK GROUND

The following genetic algorithm operations [3] are used to optimize the cluster head selection process MANET.

A. Encoding the Data

It is a string representation of the given data, which would be the mobile nodes in the network. Each mobile node have unique node id for unique representation of nodes. The genotype is a string of N positions. Each position corresponds to a particular object. The number of nodes N are randomly generated and unique node IDs are used encode the chromosome using integer permutation.

B. Initial Population

The population is randomly generated and is equal to

the no of nodes in the network.

C. Selection

The GA selects the cluster head for each chromosome and computes the fitness value for each chromosome. Due to the different set of cluster heads for each chromosome, the fitness value is different for each chromosome. According to the fitness values, roulette wheel method is used for selection of chromosome.

D. Cross Over

It is an indispensable operation to have more diverse population and depends on the rate specified that is best suited for a specific application and are found experimentally. This study uses X order 1 method with the specific crossover rate that inherits the elements between the two crossover points (inclusive) from the selected parent in the same order and position as they appeared in that parent. The remaining elements are inherited from the alternate parent in the same order as they appear, beginning with the first position following the second crossover point and skipping over all elements that are already present in the offspring.

E. Mutation

It avoids premature convergence by occasional random alternation of randomly determined bit in the given string with a specified rate. The swap method is used with the specific mutation rate that randomly selects two genes at two positions and swaps them to create the new child.

F. Replacement

The use of append method is to save the best strings into the next generation as the new set of solutions are replaced with the old solutions during the reproduction process. If it is not saved, there may lose of best strings.

G. Elitism

If the new solution is better than the previous one, it updates the current solution with the new solution.

H. Computation of Fitness Value

The fitness value is computed for each chromosome and it is explains in the fitness algorithm in the study. Based on the fitness value, the best suited chromosome is selected.

III. Related Works

They are several approaches is used to detect the intrusion node. In [1], projection distance is used to detect the malicious node of the network, using statistical decision theory to calculate the projection distance of the node. Same related data are given some training certain amount and update the data dynamically in the database and stored it.

In [2], the anomaly detection store data about the previous intrusion data and checking the database known intrusion data with the user input data. The data are same rejected or this is intrusion data to display. In [3], the agent is used to monitoring the node operation. The nodes are check the battery power and routing the data packet from one node into another node.

In section 2, we have to explain genetic algorithm operations, such selection of cluster head, crossover, mutation, replacement.

The main contribution of the fitness function select best node of the cluster .Cluster head monitoring the nodes and how to send the packets one node into another node.

IV. Genetic Cross Over Method

In genetic crossover method, calculate the fitness value of the each node. The higher fitness value is selecting the cluster head. Cluster head monitoring the node and forwarding the data into another node.

A. Initial Population

Randomly generate the initial population with the pool size being equal to the number of nodes in the network. This will produce the same number of chromosome in the form of integer strings.

B. Repeat until the Requirements met

While new pool size < old pool size, repeat steps 3-7.Repeat step 2 until the number of generation or the convergence is met.

C. Selection

Apply roulette wheel method with fitness values.

D. Cross Over Method

X order1 method with 0.02 crossover rate.

E. Mutation

The swap method with 0.08 mutation rate is used.

F. Compute Objective Function

Compute the fitness function N-H for each chromosome in the population. Where, N is total number of nodes in the network and H is the number of selected cluster heads. The chromosome with the highest fitness value is the best suited chromosome.

G. Replacement

The append method is used to save the best strings for next generation.

H. Elitism

Check if the new children are better than the current best. If so, replace the best by child.

The unique ID for N number of nodes in the network is randomly generated in the range from 1 to N. These node IDs of all N nodes are encoded in a single chromosome using integer permutation as string of integers. The initial population is randomly generated to the pool size. To achieve the completeness and uniqueness property, no duplication of node IDs are randomly and the order of placing of node IDs are randomly encoded in the chromosome. Each chromosome is traversed from the beginning till the end

to obtain cluster heads in the network that are stored in the corresponding Cluster_head_list. Each node ID is checked whether, it is not a cluster head or cluster member of another cluster head is higher than its neighbor for particular predefined transmission range. If all these three conditions are satisfied, the node is selected is selected as the cluster head and it is inserted into Cluster_head_list and its neighbor become its clusters members and they are restricted to participate in further cluster head selection process. After traversing each chromosome from the beginning till the end, each node in the chromosome should be either a cluster head or a member obtaining total cluster heads in the network stored in cluster_head_list (H) and subtracting it from total number of nodes in the network (N). Due to the different order of placing node IDs in different chromosome, different cluster_head_list are obtained for each chromosome there by obtaining different fitness values.

I. Fitness Function Process

Step 1: The fitness value is equal to 0 at the beginning.
Step 2: Repeat step 3 for each gene in the chromosome.
Step 3: Assign node to be equal t gene [3]. If a node is not a cluster head and is not a member of another cluster head weight is higher than its neighbor, select the node as a cluster head and insert its node ID to the cluster_head_list.
Step 4: If all the nodes in the chromosome are either a cluster head or a member of a cluster, the total number of selected cluster head is obtained in cluster_head_list for the chromosome. Compute the fitness value N-H or the chromosome.

J. Architecture

The Fig. 1 shows the overall process of the intrusion detection. In the anomaly detection method previously stored the intrusion data and check the user input data. Agent is used to forward the data in one node into another node. When user enters the input data, the input data is checking with the network device such as router and firewalls details. If user input data is in the database reject the data set.

The chromosome weight makes the cluster and the cluster head selection is based on the fitness value. Higher fitness value considered as head of the cluster. The individual weight is calculated to each cluster.

K. Genetic Algorithm

Genetic algorithms are inspired by Darwin's theory of evolution. It is a modern algorithm for solving any optimization problem. Solution to a problem solved by genetic algorithms uses an evolutionary process. Algorithm starts with randomly generating the set of possible solutions for an optimization problem called population. The new population will be better than the old one. Then solution which are selected to form the new solutions, are selected according to their fitness.

Fuzzy rules are used to make the baseline of the data. In anomaly detection method all data are previously stored in the database. Then user enter data check database any intrusion data is available.

L. Cross Over

Two parents produce to offspring. There is a chance that the chromosomes of the two parents copied unmodified as offspring. There is a chance that the chromosomes of the two parents are randomly recombined (crossover) to form offspring. Generally the chance of crossover is between 0.6 and 1.0.

M. Mutation

Gene of a child is changed randomly. Generally mutation is low.

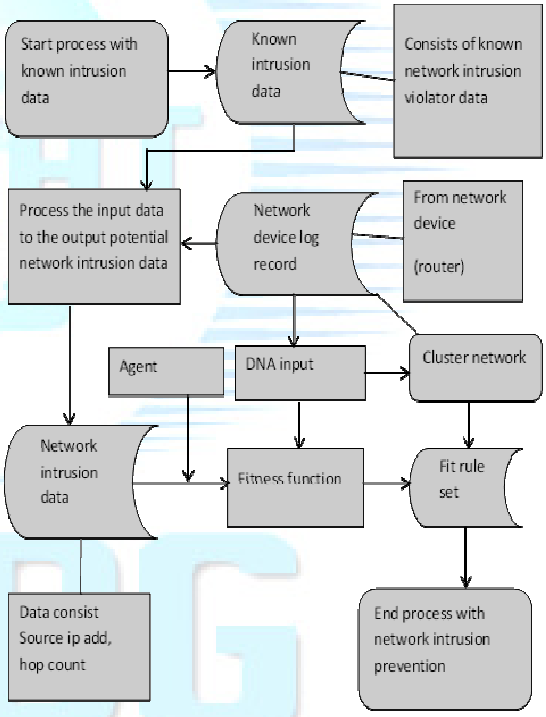

Fig. 1. Intrusion Detection

V. RESULTS

The relative weight based clustering is optimized using GA to obtain optimal number of cluster heads in the network. The metrics considered for evaluation are

1. Cluster number.
2. Re-affiliation count.
3. Cluster head changes.

1. *Cluster number*

The cluster number is the number of cluster heads in the network. The optimum number of cluster heads enhances the stability of the network.

2. *Re-affiliation count*

It is a count of number of nodes that detaches from one cluster head and attaches with another cluster head under the current dominating set re-affiliation count should be less to reduce the information exchange due to re-affiliation.

TABLE I
SIMULATION PARAMETERS

Parameter	Values
Simulation Dimension	1000×1000 m
Simulation Time	60 sec
Number of nodes	20,40,and 60 nodes
Transmission range of mobile nodes	50-150 m,200-300 m
Pause time	5 sec
Maximum speed of mobile nodes	20 $msec^{-1}$

3. *Cluster head changes*

It occurs if two cluster if two clusters heads comes into a transmission range of each other. The highest weight cluster head takes up the role of a cluster head and the other gives up its role leading to the cluster head change. Frequent cluster head change degrades the stability of the network.

A. Configuration Information

User data: n20.ahp

Data type: Integer Permutation.

Init pool entered: Random.

Chromosome Length: No of nodes in the network.

Number of trails: Run until Convergence.

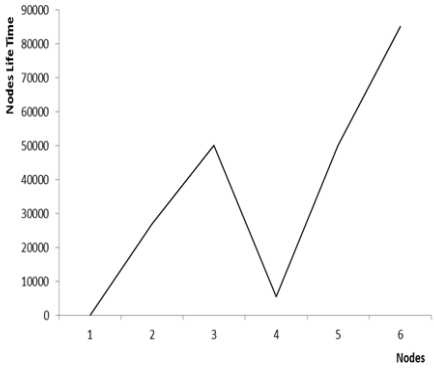

Fig 2: Nodes life time in cluster.

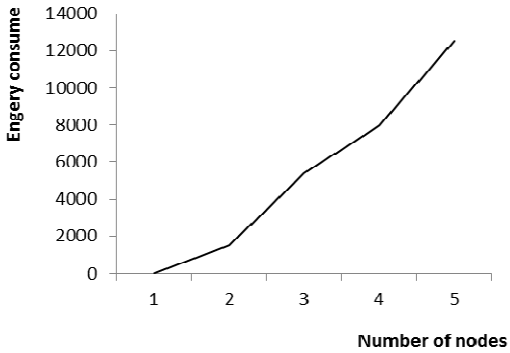

Fig 3: Nodes Energy Consumption

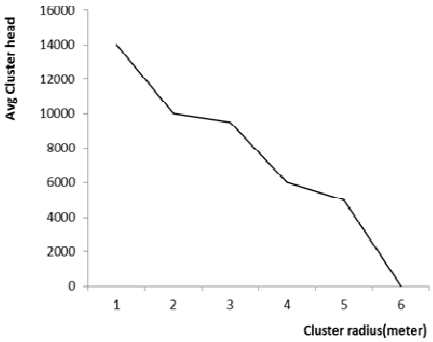

Fig 4: Cluster head changes.

VI. CONCLUSION

The Relative weight based clustering technique is enhanced by optimizing the number of cluster head using genetic algorithm approach. GA algorithm techniques were applied to optimize the cluster head handles the maximum possible number of nodes in the cluster the cluster head changes are drastically reduced leading to the increase of cluster head life time. Agent is a one type of routing protocol in this paper. In future, there is a plan to enhance dynamic learning method to reduce the cluster head changes.

REFERENCES

[1] A.Mishra, K.Nadkarni, and A.Patcha, "Intrusion detection in wireless ad hoc networks", IEEE Wireless Commun., vol.11, no.1, pp.48-60, Feb.2004.
[2] M.Chatterjee, S.K. Das and D.Turgut, 2002. WCA: A Weighted Clustering Algorithm (WCA) for mobile ad hoc networks. Cluster Compute, vol.5, pp.193-204.
[3] L.Chambers, Practical Handbook of Genetic algorithm application, vol.1, CRC Press, 1995.
[4] Er, I.I, and W.K.G.Seah, "Mobility Based d-hop clustering algorithm for mobile ad hoc networks", IEEE Wireless Commun, Networking Conf., vol.4, pp.2359-2364.
[5] B.Sun, K.Wu, and U.Pooch, "Towards adaptive intrusion detection in mobile ad hoc networks", in proc.IEEE Global Telecommunm. Conf GLOBECOM, NOV./DEC. 2004, PP.3551-3555.
[6] R.Nakkeeran, T.Aruldoss Albert, and R.Ezumalai,"Agent based efficient anomaly intrusion detection in ad hoc networks", IACSIT, vol.2, no.1, Feb.10.
[7] Yia-an Huang, W.Enke Lee, "A Cooperative intrusion detection system for ad hoc networks", ACM Workshop on security of ad hoc and sensor networks, 2003, pp.135-147.
[8] Hang Yu Yang, Li-Xia Xie, "Agent based intrusion Detection for a Wireless Local Area Network", Proceedings of the IEEE third international Conference on Machine Learning and Cybermatics, 2004, pp. 2640-2643.