A Proposed Alternative Approach for Intrusion Detection System for AD-Hoc Networks using Decision Trees and Binomial Heap

[1]Srivastava Sumit(Dr.), [2]Maheshwari Shashikant
[1]Associate Professor, Department of Computer Sc. & Information Tech., Manipal University, Jaipur
[2] Scholar M.Tech-NIS, Department of Computer Sc.& Information Tech., Manipal University , Jaipur

Abstract: - Security of Wireless Ad hoc network has a primary concern to provide protected communication between mobile nodes. When we routing some packet it can use both malicious node or authenticate node for forwarding and receiving data. Malicious node can attack like black hole, misuse of data or hacked information. Our aim is to discuss the feasibility of monitoring the node of different networks, to analyze it for providing better security. For protecting network we focus on Intrusion detection technique. We implement data mining techniques for search large amount of data according characteristic rules and patterns to detect malicious node. Using soft computing technique we find patterns, analysis node and take decision based on fuzzy-set.

Keywords: - fuzzy logic, cluster, intrusion detection technique, black-hole attack, supervised learning.

I. Introduction

An ad hoc network is a collection of wireless mobile nodes (router) dynamically forming a temporary network. The routers are free to move randomly and organize themselves. Each node can receive and transmit data accordingly. Ad hoc network have no pre-deployed infrastructure for routing packets source to destination that can be either directly or intermediate nodes in network [1]. Secure Ad hoc routing is an especially hard task to accomplish robustly and efficiently because new node can be created or deleted from networks [Fig 1]. The main objective of this paper is node security in wireless ad hoc networks the nodes can be highly mobile, thus changing the node constellation Vulnerabilities of node come from their open peer-to-peer architecture. Each mobile node in an ad hoc network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network and malicious attackers. As a result there is no clear defense. Intrusion is defined as “any set of actions that attempts to compromise integrity, confidentiality or availability”. Intrusion detection systems (IDS) are mainly used to detect malicious activity [2].

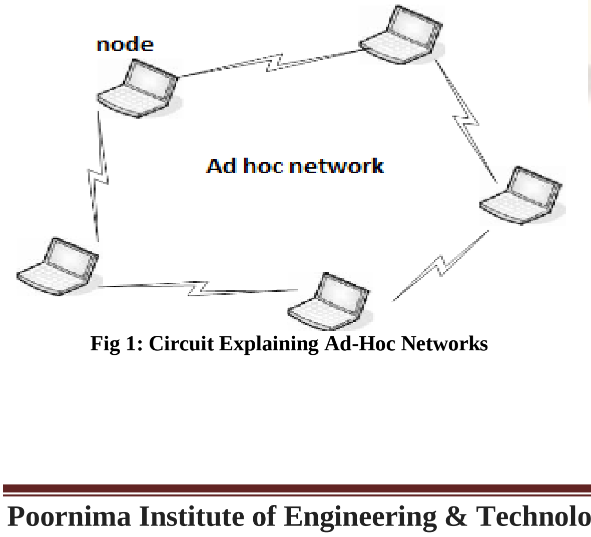

Fig 1: Circuit Explaining Ad-Hoc Networks

Past number of years, machine learning and data mining technique have received considerable attention on IDS to address the weakness of detection [3]. This has led on various supervised and unsupervised techniques. Intrusion detection is used in network by comparing and analysis nodes with behavior of system. Detection can be used to technique misuse detection and anomaly detection. This detection of normal behavior in a system usually through automated training based on actual activity of system. We have proposed k-mean clustering algorithm for detection of intruder’s activity [4].

A wireless ad hoc is to select a set of special nodes that act as a backbone for the entire communication called cluster head. Thus the nodes are grouped into clusters, and each cluster contains a single cluster head responsible for managing nodes [5]. As node can move freely and new nodes can join or leave based on soft computing learning techniques. This has led to supervised and unsupervised techniques. There are many situations in which class labels are not available and which thus require unsupervised methods. We proposed supervised training based on k-clusters.

II. Related work

The study includes strongly emphasized on Preetee Karmore [6] who proposed new Intrusion detection and also developed AODV based MANET by k-mean cluster but that cannot take decision and efficient learning on node. The problem founded is that AODV uses distance vector routing protocol which doesn’t train the node for any new packet type. We have proposed solution to take decision based on cluster using fuzzy decision tree. Ad hoc network intrusion detection system works on large scale. It monitors network node and based upon observation it categories node into normal or suspicious. Node monitoring is done at firewall, hub, and switch etc.

2.1 Data mining Techniques: -Data mining is the process of analyzing data from different perspective [8]. Classifier can be used as large number of data sets being trained. Clustering analysis algorithm can be used to construct the network model of normal or intrusion behavior. Clustering is a learning technique which divides the datasets into groups of similar objects [9].

The goal of clustering is to group sets of objects in the same cluster, while dissimilar objects are in separate clusters. Clustering can be used as analysis about node, pattern reorganization, and supervised learning. Any cluster should exhibit two main properties low inter-class similarity and high intra-class. [7]

Node analysis is concerned with predictive modeling: given some training data, we want to predict the behavior of unseen node this task also referred as training like supervised.

The first involving only labeled data for training patterns with known category labels while the latter involving only unlabeled data instead of being discarded, are also used in the learning process. In supervised clustering, instead of specifying the class labels, pair-wise link constraint corresponds to the requirement that two objects should be assigned the same cluster label, whereas the cluster labels of two objects participating should be different constraints.

We propose a new strategy for intrusion detection. It consists of three stages. Based on clustering we will trained node, we sort clusters according to their outlier factor. We label some clusters that contain percentage of the node as ‘normal’ while labeling the rest of the clusters as ‘attack’. We regard labeled clusters as model, and detect an object whether it is an attack or not by Fuzzy decision trees and membership function.

2.2 Fuzzy set theory: -Fuzzy set theory allows an object to have partial membership in more than one set. It does this through the membership function [10].Which maps from the complete set of objects X into a set known as membership space.

If X is a collection of objects denoted generically by x then a fuzzy set F in X is a set of ordered pairs:-

$F = \{(x, \mu_f(x)|x \in X\}$……………………….(eq 1.)

$\mu_F(x)$ is called membership function of x in F which maps to membership space M [12].

2.2.1Fuzzy decision tree: -Fuzzy logic used here fuzzy decision tree. A decision tree is a tree where each non-terminal node represents a test or decision with composite concept, i. e. concepts constructed from root concepts using AND, OR, NOT on the considered data item. Choice of a certain branch depends upon the outcome of the test. To classify a particular data item, we start at the root node and follow the assertions down until we reach a terminal node (or leaf). A decision is made when a terminal node is approached. Terminal nodes are labeled with what are referred to as root concepts.

And each root concepts has a fuzzy membership function assigned to it. The membership function for composite concepts are constructed from those assigned to root concepts using clustering data. Decision trees can also be interpreted as a special form of a rule set, characterized by their hierarchical organization [10, 11].

To build node we used binomial heap structure. Because using this we can easily insertion and deletion of node and can check behavior of node [13]. A decision tree is a classification technique which represents set of rules, and different classes, from given data set that distinct subset known as training set or test set. The training data is used to build classifier and the test data find accuracy of classifier.

III. Proposed Algorithm

3.1 Learning technique: - There are several classification algorithms among which we as proposed supervised learning, Where the nodes are labeled with predefined classes’ i.e. learning based on training data In unsupervised learning, where algorithm is provided with data points only but not labels means the learning without training data. That’s I proposed supervised learning. The accuracy of supervised algorithm deteriorates significantly if unknown attacks are present in test node. But using fuzzy set it can handle.

We proposed solution for intrusion detection. When new node comes first we check node which is present in cluster or not. If it is present then add into our network otherwise we make new node based on decision tree and will apply learning technique on it. The supervised algorithms are evaluated separately on node with known and unknown attacks. The supervised algorithm is general excellent classification accuracy on node with known attacks. We trained our node on basis of supervised learning technique and can take decision using fuzzy decision tree. We create binomial tree for successful node creation as shown in the Fig 2.

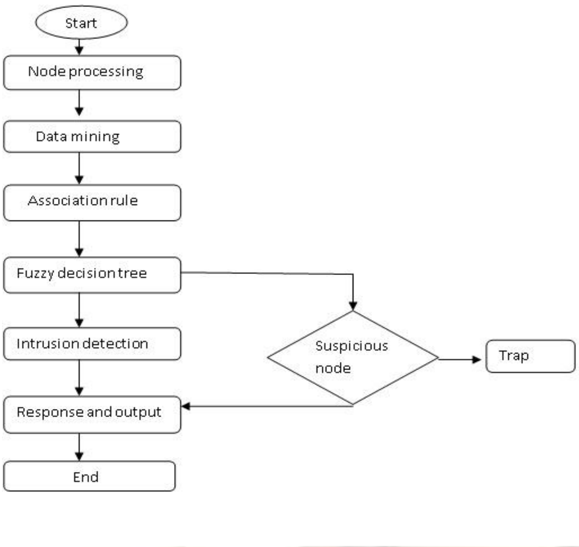

Fig 2: Binomial Tree for Node Creation

IV. Conclusion

Intrusion detection is varied field of the network security research; it is new kind of defense technology of network security. Thus the approaches working for IDS should be enhancing the approaches for making the nodes to be intelligent. The Technique for intrusion detection mechanism emphasized in this paper utilizing cluster data mining technique, fuzzy logic, and supervised learning techniques or the techniques related to Soft Computing. We have proposed architecture with clustering, decision tree, and learning method. Our proposed intrusion detection architecture is designed to detect malicious node or normal node in mobile ad hoc network. The future work can further improve detection rate and make secure network by running the decision trees for parallel architecture.

V. References:-

[1] Sarkar S. K., Ad hoc mobile wireless network Chapter 1, Auerbach publications.

[2] ZhouLidong, Securing Ad Hoc Networks, Cornell University, IEEE network, special issue on network security, November/December, 1999

[3] Nadiammai G.V., A Comprehensive Analysis and study in Intrusion Detection System using Data Mining Techniques. International Journal of Computer Applications (0975 – 8887), Volume 35– No.8, December 2011

[4] MunzGerhard, Traffic anomaly detection using k-means clustering, Wilhelm Schickard Institute for Computer Science, University of Tuebingen, Germany

[5] DattaAjoy k., A self- stabilizing Link-Cluster algorithm in Mobile ad hoc network, ISPAN '05 Proceedings of the 8th International Symposium on Parallel Architectures, Algorithms and Networks, Pages 436 – 441,IEEE Computer Society, Washington, DC, USA©2005

[6] KarmorePreetee K., Detecting Intrusion on ADOV based mobile ad hoc network by k-mean clustering method of data, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1774-1779

[7] PratimaDepa, pattern recognition for cluster identification problem, Special Issue of International Journal of Computer Science & Informatics **(**IJCSI), ISSN **(**PRINT**)** : 2231–5292, Vol.- II, Issue-1, 2

[8] ModiShweta, the role of data mining in design and implementation of intrusion detection systems. International Journal of Computer Technology and Electronics Engineering (IJCTEE), Volume 1, Issue 2

[9] BhartiKusumKumari, Intrusion Detection using clustering, Special Issue of IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], 3-5 August 2010

[10] Smith F. James, naval Research laboratory, fuzzy logic resource manager evolving fuzzy decision tree structure adapt in real time. Proceedings of the Sixth International Conference of Information Fusion - FUSION 2003, Volume: 2

[11] Joshi Manish, Amity University, classification, clustering, and intrusion detection system. International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, Mar-Apr 2012, pp.961-964

[12] Zimmerman H.J., Fuzzy set Theory and its application, chapter-1, Kluwer Academic Publishers Group, Boston, 1991.

[13] Coreman Thomas, Introduction to Algorithm, chapter-19, Tata Mac-Graw Hill Publication