iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 1 **Issue:** V **Month of publication:** December 2013

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Analysis of Artificial Neural Networks Based Intrusion Detection Systems for Mobile Ad Hoc Networks

Alka Chaudhary[#], V.N.Tiwari*, Anil Kumar[#]

[#]*CSE, Manipal University jaipur, India*

[*]*E&C, Manipal University jaipur, India*

Abstract— In mobile ad hoc networks, Intrusion detection system is known as the second line of defense because prevention based techniques are not a good solution for ad hoc networks due to its complex characteristics. For the security point of view, many intrusion detection systems have been proposed to mobile ad hoc networks in literature. This paper analyzed the proposed artificial neural networks based intrusion detection systems and also discussed their applicability in mobile ad hoc networks.

Keywords— Mobile ad hoc networks (MANETs), MANETs Security issues, Intrusion detection system (IDS), IDS components, artificial neural networks (ANNs).

I. INTRODUCTION

Mobile ad hoc networks are very flexible network in terms of communication because there is no need of predefine infrastructure for communication between the mobile nodes. Some characteristics of MANETs such as communication via wireless links, resource constraints (such as bandwidth and battery power), cooperation between the nodes due to communication protocols and dynamic topologies make it more vulnerable to attacks [1].

Intrusion detection is a security technology that attempt to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges. An Intrusion detection system dynamically monitors a system and user actions in the system to detect intrusion [2].

The basic functionality of IDS depends only on three main components such as data collection, detection and response. The data collection component is responsible for collect the data from various data sources such as system audit data, network traffic data, etc. Detection module is responsible to analysis of collected data to detect the intrusions and if detection module is detected any suspicious activity in the network then initiates the response by the response module. There are mainly three detection techniques such as misuse based, anomaly based and specification based techniques presented in the literature [3].

Misuse-based detection systems detect the intrusions on the behalf of predefined attack signature. Second intrusion detection technique is Anomaly-based detection technique. It detects the intrusion on bases of normal behavior of the system. The third technique is specification - based intrusion detection. In this detection technique, first specified the set of constraints on a particular protocol or program and then detects the intrusions at the run time violation of these specifications.

This paper emphasized on proposed neural networks based intrusion detection system in mobile ad hoc networks. Artificial neural networks are very important method to differentiate normal and malicious nodes in the MANETs. ANNs have the ability to detect intrusions with high detection rate and forecasting the unknown patterns or learning capability [7]. In the rest of paper are organized as

follows: in section II analyze the proposed neural networks based intrusion detection system and section III presents the conclusion in terms of results.

II. ARTIFICIAL NEURAL NETWORKS BASED INTRUSION DETECTION SYSTEMS IN MANETS

This section is going to present the proposed artificial neural networks based intrusion detection systems in mobile ad hoc networks. Table 1 presented the detailed description of proposed artificial neural networks based intrusion detection systems.

A. SVM based intrusion detection system in MANETs:

In this paper Hongmei Deng et al. [4] proposed support vector machine based intrusion detection system that emphasized on the security issues of network layer in wireless ad hoc networks. It is suitable for real time intrusion detection. They have also proposed two distributed system detection models which are distributed hierarchical model and completely distributed model.

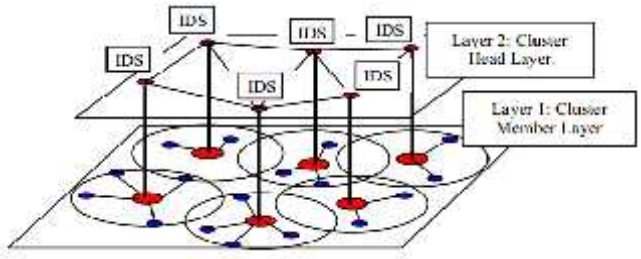


Figure 1: A Distributed Hierarchical Detection Model [4]

They considered Ad hoc On-demand Distance Vector (AODV) routing protocol for proposed models. Whole network divided into the clusters.

In distributed hierarchical model have two layers: first layer for cluster member layer and second layer for cluster head layer as shown in figure 1. Actually cluster head of a particular cluster have only capability to take decision and give local response and then help of all clusters cluster head together raised the global response.

But in this approach no security provided for cluster head.SVM intrusion detection approach basically worked on second layer. They have taken two attack types of Dos attack and provide higher detection accuracy.

B. Neural network and Watermarking based IDS on MANETs:

Aikaterini Mitrokotsa et al. [5] first proposed neural network based intrusion detection system which provided the information visualization for achieving direct response in case of possible intrusions and they used watermarking techniques for the authentication of information visualization.

The proposed IDS architecture is composed of multiple local IDS agents that are responsible for detecting the possible attacks on MANETs as shown in figure 2. The components of local IDS are – Data collector (local audit data and activity logs); Intrusion detection engine; Intrusion response engine.

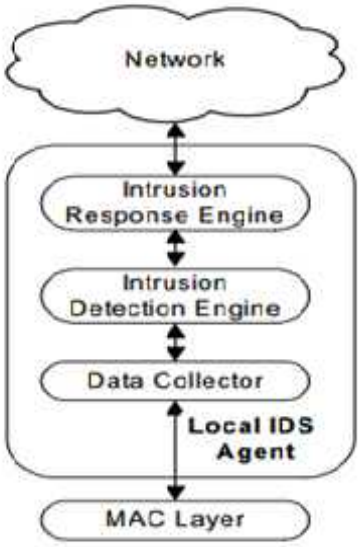


Figure 2: Intrusion detection Architecture [5]

The Intrusion detection engine is responsible for detecting anomaly from local audit data. In this SOM (class of neural network) used to produce output in the form of visual representation of classification performed.

They used eSOM classifier for classifying the normal and abnormal data which based on MAC layer features and after that watermarking technique applied on local eSOM map (normal data) for authentication. Intrusion response engine are

responsible for sending local (one hop neighbors of a node) and global alarm (all nodes in a node transmission range).

They used combined watermarking techniques (Lattice and Block-Wise method) for authentication of eSOM map and evaluated their system performance on the ns-2 simulator under the packet dropping attack. But it is not evaluated under the high mobility and high traffic activity. Proposed IDS using eSom needs to be trained in regular interval. So it caused overhead affects the energy efficiency of the algorithm.

They considered limited number of attacks. In their future work included to develop intrusion detection engine which can employ various routing protocols and can detect various types of attacks. This system may be provided computation complexity in generation and verification of digital signature

C. Back Propagation Network (BPN) Approach based IDS for MANETs:

Min-Hua Shao et al. [6] presented an intrusion detection system which is based on the cluster-based cooperative back propagation network approach. The proposed approach used anomaly based detection method for the detection of unknown attacks but the selected features for collecting the data are too limited in this paper.

In implementation point of view, this paper emphasized on few attacks such as changing serial number attack and packet drop attack. This paper also showed the comparison between BPN and finite state machine.

D. *Neural network based IDS in MANETs:*

Zahra moradi et al. [7] also proposed the neural network based intrusion detection system for MANETs. They can efficiently detect nodes under DoS attack. For this purpose they are selected Feed Forward Back Propagation network type.

For the data collection based selected features are too limited for the detection of unknown attacks. Implementation point of view, this paper used ns-2 simulator and MATLAB toolbox.

IDS	Researcher	year	Data Source	Detection Technique	Addressed attack type	Contribution	Other manet IDS issue
SVM based IDS[4]	Hongmei Deng et al.	2003	Audit data	Misuse based detection	black hole attack and Frequent False Routing Requesting (FFRR).	Applied new category of machine learning method for classify normal and abnormal data patterns for wireless ad hoc networks	Not suitable for any routing protocol and any attack type. Not provide clusterhead security
Neural network and Watermarking based IDS [5]	Aikaterini Mitrokotsa* , Nikos Komninos et al.	2007	local audit data and Logs of network traffic	Misuse based detection	Packet dropping attack	First used neural network and watermarking approach for MANETs security Neural approach provided information visualization for achieving response of intrusion Watermarking technique used for authentication of	IDS using eSom needs to be trained in regular interval. So it caused overhead affects the energy efficiency of the algorithm. Cannot detect different type of attacks.
Back Propagation Network (BPN) Approach[6]	Min-Hua Shao Ji-Bin Lin Yi-Ping Lee	2010	Packet related data	Anomaly detection method	Modify serial number attack, Packet drop attack	Back Propagation Network (BPN) Approach used for anomaly based detection Make the comparison between BPN and finite state machine detection approach	packet related feature is too limited
Neural network based IDS [7]	Zahra moradi, Mohammad Teshnehlab	2012	Logs of network traffic	Anomaly based	Dos type attack	Neural networks based approach is used to detect a kind of DoS attack.	Limited features selected for data collection. Concentration only one specific attack Consider distributed architecture type IDS

Table 1: Proposed artificial neural networks based Intrusion detection systems in MANETs

III. CONCLUSION

In this paper, we have analyzed neural networks based intrusion detection system for mobile ad hoc networks. As a result, there are few IDSs proposed in literature which are based on ANNs. These proposed IDSs have emphasized only few features for data collection and few specific attacks in MANETs. For the future aspect, there is need for new IDS which can cover all features for data collection towards detection of all attacks.

REFERENCES

[1] Y. Li and J. Wei., "Guidelines on selecting intrusion detection methods in MANET", *In Proceedings of the Information Systems Educators Conference*, 2004.

[2] Bo Sun and Lawrence Osborne: Intrusion detection techniques in mobile ad hoc and wireless sensor network. In: IEEE Wireless Communications, 1536-1284, 2007.

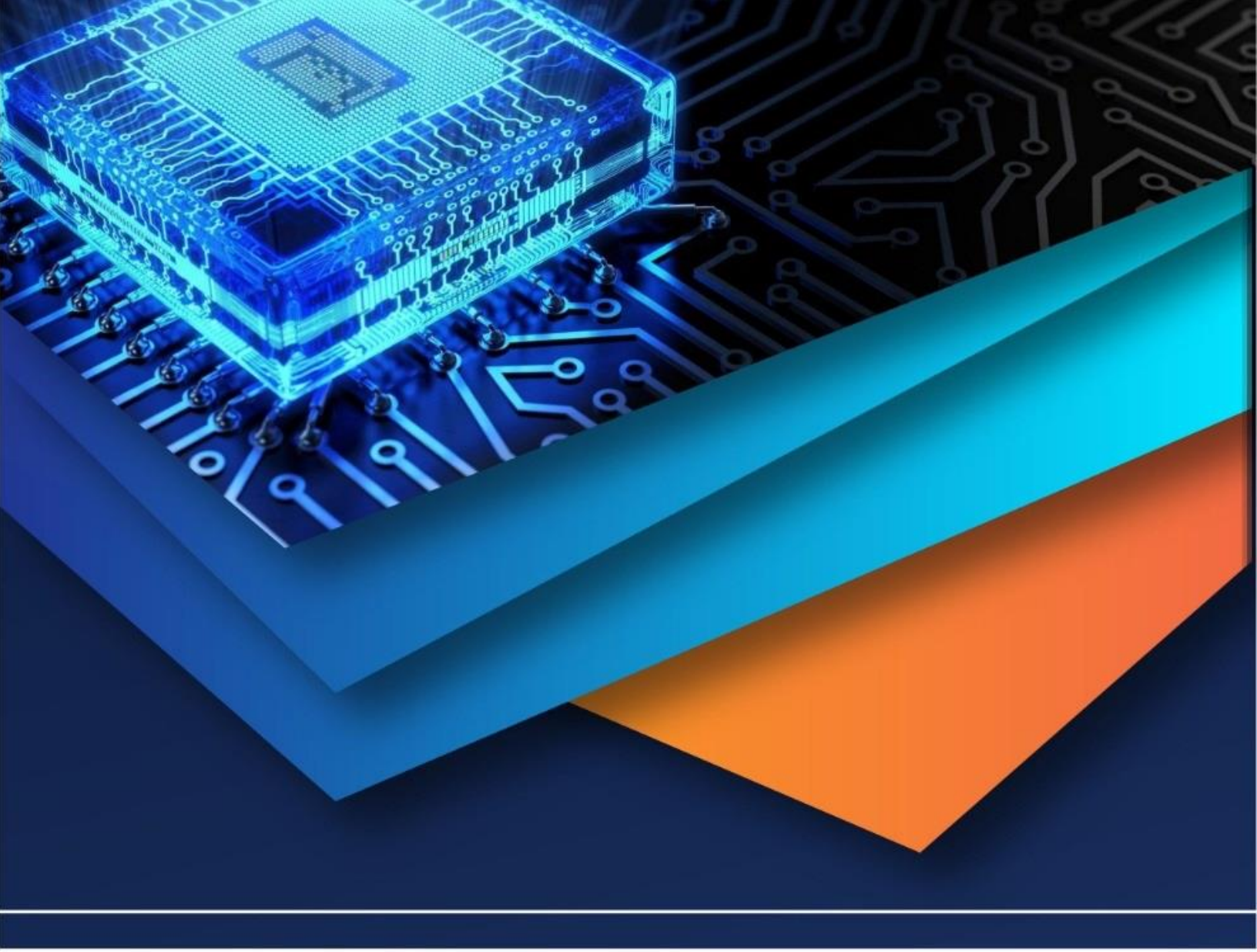
[3] R. Heady, G. Luger, A. Maccabe, and M. Servilla, "The architecture of a network level intrusion detection system", Technical report, Computer Science Department, University of New Mexico, August 1990.

[4] H. Deng, Q. Zeng, and D. P. Agrawal, "SVM-based Intrusion Detection System for Wireless Ad Hoc Networks", In Proceedings of the IEEE Vehicular Technology Conference (VTC'03), Oct. 2003, Orlando, Florida, USA, pp. 2147-2151.

[5] A. Mitrokosta, N. Komninos and C. Douligeris, "Intrusion Detection with Neural Networks and Watermarking Techniques for MANETs", In Proc. IEEE International Conference on Pervasive Services, pp 118-127, July 2007.

[6] Min-Hua Shao, Ji-Bin Lin; Yi-Ping Lee, "Cluster-based Cooperative Back Propagation Network Approach for Intrusion Detection in MANET in IEEE 10th International Conference on Computer an Information Technology (CIT), 2010.

[7] Zahra moradi Mohammad Teshnehlab Amir Masoud Rahmani, " Implementation of Neural Networks for Intrusion Detection in MANET", IN International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT), 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY