Journal of Mathematical Problems, Equations and Statistics

E-ISSN: 2709-9407
P-ISSN: 2709-9393
JMPES 2023; 4(1): 01-04

www.mathematicaljournal.com
Received: 05-10-2022
Accepted: 07-11-2022

DS Pathania
GNDEC Ludhiana, Punjab, India

Pardeep Kumar
CT University Ludhiana, Punjab, India

Corresponding Author:
DS Pathania
GNDEC Ludhiana, Punjab, India

A hybrid approach for intrusion detection system using and artificial neural network

DS Pathania and Pardeep Kumar

Abstract
MANET is an infrastructure-less ad-hoc network. It is a collection of mobile nodes that are connected in an arbitrary and dynamic manner. ANN (Artificial Neural Network) is a type of Machine Learning scientific and statistical model that is used by computer systems in order to perform a task without involvement of explicit intrusion, rather than relying on interference and patterns instead. As there is node mobility that can impose different security issues, MANETs are found more susceptible in security provision. In order to resolve this security issue, some authentication and encryption techniques can be proposed for the first-line defence in order to mitigate the security risks. However, complete eradication of these types of risks is next to impossible. For the second-line defence, the necessity of an Intrusion Detection System (IDS) is essential in this case. IDS can be referred as a method tool or resource that can help to detect access and warn for any activity of unapproved or unauthorised network activity. Thus, it is important to deploy a hybrid network using ANN based and data mining based IDS systems that can enable the system in making decisions on intrusion in a mobile environment. This paper is going to present a hybrid model for IDS using ANN and data mining approaches.

Keywords: MANET, intrusion detection system IDS, Artificial Neural Network (ANN)

1. Introduction
MANET being a moving ad-hoc network consists of a series of autonomous nodes which make a multi-hoc radio and dynamic network in a cooperative and decentralized way. Due to the unique features this technology is being utilised to support the communication in those environments where it is next to impossible to deploy any high infrastructural network. These environments can be considered as disaster recovery commercial sectors, sites and military battlefields. MANET is considered as very susceptible to different types of attacks such as routing, eavesdropping, packet modification due to the dynamic topology and node mobility. Thus, it is important to deploy a hybrid network using ANN based and data mining based IDS systems that can enable the system in making decisions on intrusion in a mobile environment.

2. Problem detection
The attacks in MANET can be classified into two major categories such as active and passive attacks. A passive attack includes the exchange of data in a network without creating any interruption in the communication activities while active attacks includes the interruption in the communication and information, manufacturing and modification that can cause the normal functionality of MANET. The examples of passive attacks are traffic analysis, eavesdropping, and traffic monitoring. The attacks can be also differentiated by internal and external attack.

2.1 Blackhole attack
There are mainly two fundamental properties of black-hole attack. Firstly, the node of black-hole network uses AODV protocol in order to advertise itself that it is having a reliable route from source to destination node in spite of having a spurious route with the probability of intercepting packets. Secondly, the attacker can absorb the intercepted packets rather than forwarding it further. However, it can be considered that the attackers are well-known regarding the risk of running that monetization and exposition can be done by the neighbouring nodes. In this type of attack, the attacker can modify or detect the intercepted packets in a way that the suspicious activities of wrong activities remain untouched-hole attack.

2.2. Wormhole attack

In a network environment, the attacker records the data packets and forwards them through a tunnel to another network environment. These tunnels are considered a wormhole that acts between two attackers. The wormhole attack can be performed through one single node but most of the time, two or more nodes that are obviously malicious are connected through wormhole links. In the following fig (fig 1) a wormhole attack is displayed.

3. Improvement in prediction accuracy

In the application of data mining in the intrusion detection network, the detection approaches are generally implemented offline as the learning algorithms possess a large amount of archived data. These approaches are fundamentally used in intrusion detection in an offline manner. The intrusion detections should be performed in real-time as soon as the taking place of intrusion happens in order to mitigate the security compromises issues. In order to develop a real-time intrusion detection system, the data mining based IDS approaches are developed in order to identify the potential intrusion in the early stage.

The architecture of data mining based IDS includes a series of detectors and sensor nodes, a model generating compound and a data warehouse. This modified architecture can not only support data collection, sharing and evaluation processes but also includes model generation, data achieving and data distribution. In order to deal with this heterogeneity issue, XML coding is utilised for each of the components so that the data exchange can easily happen. However, in this architecture the detectors is called 'black-end' detectors as the workload is distributed to various detectors in order to perform the analysing events in a parallel manner.

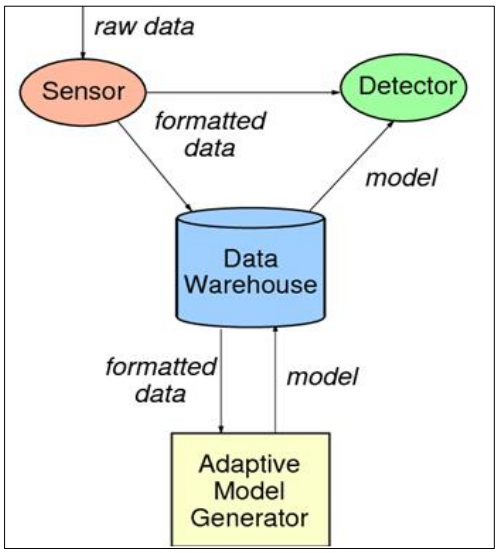

Fig 3: Architecture of Data mining based IDS

3.1 Decision tree algorithm

This algorithm is called J-48 in the Weka Data mining. The development of the algorithm has emerged as ID3. This algorithm utilises the conquer and divide approach and normalization of operation is involved in this type of algorithmic structure. The values from the information are calculated and is utilised in forming the ratio in this algorithm. In this case, the lower trees can be formed in the decision tree and it is also possible to transform these lower trees into other levels. In this kind of decision tree algorithm, in order to detect and delete issue-oriented data from a large data set, a branch pruning is done effectively to reduce the rate of error. In this tree construction process, one single node can be detected and thus this starts processing. If all the samples are found of one class then the corresponding node is determined as a leaf and acts as a representative of a class. On the other hand, if it is found that the samples are from different classes, then the best segmentation is taken into account and the branching process continues.

In the below fig (fig 4) the creation of random vectors occurs in the initial stage, then the random vectors are used to establish different decision trees and in the step three the decision tree is combined with a new sub-tree. Decision tree algorithm for performing data mining operation.

4. Development and design ids in manet

With the continuous monitoring of the audit trail traffic, detection of the malicious performances or attacks can be identified in the network system or the standalone network system activities. The ad-hoc or mobile networks in the MANET system involve the wireless nodes (mobile) that are dynamically arranged in a self-organized manner. In order to use the MANETs in a safe manner, the highly structured security mechanisms are constructed. The intrusion can be detected through the classification of the algorithms as 'normal' and 'abnormal' in order to easily discriminate against the intrusions. Thus, the development of IDS has occurred in MANET.

4.1 Stand-alone system

In order to determine intrusion in the system, the IDS tools run individually with independent nodes. All the decisions regarding the specific activity solely dependent on the node and also there is no collaboration is observed among the nodes in the same networking environment. Thus, the information transformation does not occur in such a network and also alert information is not transferred as one node has no idea about the activities of the other nodes due to the lack of collaboration among the nodes. Thus, the model is not effective due to the limitation. However, this model is effective in those systems where the installation of IDS has already occurred. As compared to the multi-level network structure, this system is only suitable in the single-layered network. As the single node information is not adequate for the detection of the intrusion, thus for building MANET IDS, this approach is not selected.

4.2. Cooperative and distribution system

In this model, each of the nodes consist of an individual IDS agent that can detect the intrusions. Moreover, each node has the ability to collaborate with the neighbouring nodes in order to globally detect the intrusions. Whenever any in determination is evident, a broader and high level of search is required. However, when the intrusion occurs in such a system, the local or global responses are issued by the IDS agent. In this process each of the node responses in the process of intrusion identification as an IDS agent is involved in each of the nodes. In this regard, it can be considered that an IDS agent is able to collect and detect the local data for the identification of the attack in a network. Thus, this system is suitable for IDS based MANET development in a flat network.

5. ANN Based IDS

Table 1: Supervised ANN based IDS taxonomy

Approaches	Advantages or characteristics	Challenges
Artificial Neural Network or ANN	Updating new information is difficult. Novel intrusion cannot be detected. The features are based on the foundation of human brains. It comprises three phases such as data collection, training and examination to detect the attacker. It is able to perform in noise, incomplete and limited dataset. The leaning is easy and does not require reprogramming.	Higher time for data processing. Very slow model training process that may not be appropriate for the high mobilized networks. During the training data over fitting happens.
Decision tree	· It is suitable for the larger data sets. · The accuracy for the detection is higher.	· High computation is involved in the construction of the decision tree.

5.1 Feature selection

This is an important step for extraction and selection of the crucial parameters from a larger data set. In the initial stage of the detection system establishment, the analysis of probabilistic behaviour is done that includes the mobility of nodes in the network atmosphere. However, the missing of the specific intrusion-related features can make it difficult in the discrimination against the normal flow of the potential traffic. Thus, the mission of intrusion-related objectives may create errors and thus can affect the IDS functions. Thus, for creating better detection accuracy, the researchers use the hybrid model of ANN and data mining in the development of MANET. It is very important to for researchers to have the better system for the better accuracy so that IDS functions should not get affected.

5.2 The architecture of ANN based detection model

The ANN based detection models fundamentally classify and learn the features of the nodes' observed behaviour by the proper utilization of the detection algorithm. In this case, the appropriate and suitable features are taken into account as input. The module design of MANET system requires the best energy efficient features. Thus, in order to save the energy, the IDS models should consume very little energy in order to achieve the targeted performance from the MANET system. In this process each of the node responses in the process of intrusion identification as an IDS agent is involved in each of the nodes.

6. Hybrid model of ANN

Thus, the hybrid model of ANN can efficiently detect the intrusion in the MANET system. On one hand, the architecture of data mining based IDS can not only support data collection, sharing and evaluation processes but also includes model generation, data achieving and data distribution. The architecture is designed as independent from model representation and format of sensor data. In this architecture, the model can be anything rather than a neutral network. In order to deal with this heterogeneity issue, XML coding is utilised for each of the components so that the data exchange can easily happen. On the other hand, the ML (Machine Learning) based ANN tools response in the process of intrusion identification as an IDS agent is involved in each of the nodes. Thus, for creating better accuracy in the MANET tools, most of the researchers use a hybrid model of ANN and Data Mining.

7. Objectives covered in this research paper

In this present research work, the better detection facility of the MANET for the intruders is performed and it has been evaluated in a detailed manner how the hybridization of Ann and data mining process in the MANET optimize the performance level in the detection of the malicious activities.

In the future, for enhancing the efficiency of the MANET, fuzzy logic can also be used along with the ANN model for achieving higher accuracy in the detection of malicious activities or attackers in the very initial stage. This process will include CS algorithms and decision tree.

8. References

1. Wu B, Lin F, Zhou J. A novel routing with data mining is disconnected mobile ad-hoc networks", 2010 17th International conference on Telecommunication, Doha, 2010, p, 755-762.
2. Purwar A, Singh SK. Issues in data mining: A comprehensive survey," 2014 IEEE International conference on computational intelligence and computing Research, Coimbatore, 2014, p. 1-6.
3. papadimitratos P, Haas ZJ. Secure data communication in mobile ad hoc networks", in IEEE Journal on selected Areas in communication, 2006 Feb;24(2):343-356.
4. Fiore M, Ettore Casetti C, Chiasserini C, Papadimitratos P. Discovery and verification of Neighbor Positions in Mobile Ad Hoc Networks," in IEEE Transactions on mobile computing, 2013 Feb;12(2):289-303.
5. Kumar D, Srivastava A, Gupta SC. Performance comparison of pro-active and reactive protocols for MANET, 2012 International Conference on Computing, Communication and Application, Dindigul, Tamilnadu, 2012, p. 1-4.
6. Venkatesan TP, Raja Kumar P, Pitchaikkannu, A. Overview of Proactive Routing Protocols in MANET," 2014 Fourth International conference on Communication systems and Network Technologies, Bhopal, 2014, p. 173-177.
7. Chaubey N, Aggarwal A, Gandhi S, Jani KA. Performance Analysis of TSDRP and AODV Routing Protocol under Black Hole Attacks in MANETs by varying Network Size," 2015 Fifth International conference on Advanced Computing & Communication Technologies, Haryana, 2015, p. 320-324.
8. Rajendra PP Shivashankar. Multitier every system review on secure intrusion detection system IN MANETs,"2017 2nd IEEE International conference.
9. Nadeem A, Howarth MP. A survey Of MANET Intrusion Detection & amp; Prevention Approaches for network Layer Attacks ," in IEEE Communications Surveys & Tutorials. 2013 Fourth Quarter;15(4):2027-2045.
10. Zexi C, Feidan H. Cuckoo search," 2017 3rd IEEE International Conference on Computer and Communication (ICCC), Chengdu, 2017, p.2241-2246
11. Zexi D, Freidan H. Cuckoo search algorithm for solving numerical integration", 2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER) , Shenyang, 2015, p. 1508-1512.

12. Peng J, Li K, Irwin GW. A New Jacobin Matrix for Optimal Learning of Single-Layer Neural Networks, in IEEE Transaction on Neural Networks. 2011 Nov;22(11):1823-1836.
13. Oong TH, Isa NAM. Adaptive Evolutionary Artificial Neural Networks for Pattern Classification, in IEEE Transactions on Neural Networks, 2011 Nov;22(11):1823-1836.
14. LV Y, Liu J, Yang T. Comparative studies of model performance based on different data sampling methods, In IEEE Control and Decision Conference (CCDC), 2013 25th Chinese, 2013 May, p. 2731-2735.
15. Xie H, Shang F. The study methods for post-pruning decision trees based on different based on comprehensive evaluation standard, 2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Xiamen, 2014, p. 903-908.
16. Juan Sun, Xi-Zhao Wang. An initial comparison on noise resisting between crisp and fuzzy decision trees, 2005 International Conference on Machine Learning and Cybernetics, Guangzhou, China. 2005;4:2545-2550.
17. Bari MA, Kalkal S Ahmed. A Comparative study and Performance Analysis of Routing Algorithms for MANET."In Springer Computational Intelligence in Data mining, Singapore, 2017, p. 333-345.
18. Srivastava P, Kumar R. A Timestamp-Based Adaptive Gateway Discovery Algorithm for Ubiquitous Internet Access in MANET. In Springer Next-Generation Network, Singapore, 2018, p. 153-162.
19. Patel NJK, Tripathi K. Trust Value based Algorithm to Identify and Defence Grey-Hole and Black –Hole attack present in MANET using Clustering Method," International Journal of Scientific Research in Science, Engineering and Technology. 2018, p. 281-287.
20. Raina V, Kumari S, Bhattacharya PP, Jain VK. The Evaluation and Detection of Sinkhole Attack by Implementing Genetic Algorithm in MANET, "Mody University International Journal of computing and Engineering Research, 2017, 75-82.
21. Rajesh MV, Gireendranath TVS, Murthy JVR. A Novel Energy Efficient Cluster Based Routing Protocol for Highly Dense MANET Architecture, International Journal of Computational Intelligence Research, 2017, p. 719-744.
22. Cho J, Chen I, Feng P. Effect of intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile Ad Hoc Networks", in IEEE Transactions on Reliability. 2010 March;59(1):231-241.
23. Boppana RV, Su X. On the Effectiveness of Monitoring for intrusion Detection in Mobile Ad Hoc Networks", in IEEE Transactions on Mobile computing. 2011 Aug;10(8):1162-1174.
24. Ma C, Fang Z, Wang L, Li Q. A Novel Intrusion Detection Architecture for Energy-Constrained Mobile Ad-hoc Networks", 2009 International Conference on Multimedia Information Networking and Security, Hubei, 2009, p. 366-369.
25. Poongothai T, Durshaiswanu K. Intrusion detection in Mobile Ad hoc network using machine Learning approach", International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai,2014, p. 1-5.
26. Authur MP. An SVM- based Multiclass IDS for Multiclass Routing Attacks in Mobile Ad Hoc Networks." 2018 International Conference on Advances in computing, communications and Informatics (ICACCI), Bangalore, 2018, p. 363-368.
27. Shams EA, Rizaner A. A novel support vector machine based intrusion detection system for mobile ad hoc networks, Wireless Networks, 2018, p.1821-1829.