# NETWORK FRAUD DETECTION USING ARTIFICIAL NEURAL NETWORKS

*[1]Ikechukwu F. C. Onah, [2]H. C. Inyiama*
*Department of Computer Engineering, Enugu State University of Science & Technology, Enugu*
*Department of Electronics and Computer Engineering, Nnamdi Azikiwe University, Awka*
*E-mail: ikonah@yahoo.co.uk, hcinyiama2002@yahoo.com*

## ABSTRACT
The constantly changing nature of network attacks requires a flexible defensive system that is capable of analyzing the enormous amount of network traffic in a manner which is less structured than rule-based systems. In this research paper, the analytical strengths of Artificial Neural Networks have been proposed to identify the typical characteristics of system users and determine statistically significant variations from the user's established behaviour. The advantages and limitations of neural nets are presented. The paper went on to explain the training process and learning paradigms of Artificial Neural Networks. An Artificial Neural Network agent can be deployed in a multi-agent architecture for the purpose of observing, gathering and recording data that can be used in detecting frauds within a network.
Keywords: Fraud detection, neural networks, Intrusion detection, Fraud classifiers.

## INTRODUCTION
Rule-based fraud and intrusion detection systems have been demonstrated to be relatively effective if the exact characteristics of the attack are known. Statistical Analysis involves statistical comparison of current events to a predetermined set of baseline criteria. The technique is most often employed in the detection of deviations from typical behavior and determination of the similarity of events to those which are indicative of an attack.

However, network intrusions are constantly changing because of individual approaches taken by the attackers and regular changes in the software and hardware of the targeted systems. Because of the infinite variety of attacks and attackers even a dedicated effort to constantly update the rule base of an expert system can never hope to accurately identify the variety of intrusions.

Artificial neural networks offer the potential to resolve a number of the problems encountered by the other current approaches in the detection of computer intrusions, viruses and malicious software in computer networks. They were specifically proposed to learn the typical characteristics of system users and identify statistically significant variations from the user's established behavior that may be an indication of fraud. Neural networks combine multiple Artificial Intelligence Technologies to identify suspicious activity and effectively classify patterns. Non-intrusive implementation and easy integration with standard protocols - XML, SOAP/WEB services - is also possible.

Neural networks conduct an analysis of the information and provide a probability estimate that the data matches the characteristics which it has been trained to recognize. While the probability of a match determined by a neural network can be 100%, the accuracy of its

decisions relies totally on the experience the system gains in analyzing examples of the stated problem. The neural network gains the experience initially by training the system to correctly identify pre-selected examples of the problem. The response of the neural network is reviewed and the configuration of the system is refined until the neural network's analysis of the training data reaches a satisfactory level. In addition to the initial training period, the neural network also gains experience over time as it conducts analyses on data related to the problem.

Some of the reasons why ANN is considered an ideal application for fraud detection include:

1) Neural networks are adaptive, i.e., they can take data given for training or initial experience and learn from it with a high degree of accuracy. The ability of the neural network to "learn" the characteristics of misuse attacks and identify instances that are unlike any which have been observed before by the network is probably the most important advantage. The network would also gain the ability to apply this knowledge to identify instances of attacks which did not match the exact characteristics of previous intrusions. The probability of an attack against the system may be estimated and a potential threat flagged whenever the probability exceeds a specified threshold.
2) Flexibility - Neural networks can generalize, i.e., they can correctly process data that only broadly resembles the data they were trained on originally. Generalization is useful in applications because real world data is noisy. Self-Organization enables ANN to create its own organization or representation of the information it receives during learning time. Similarly, they can handle imperfect and incomplete data, providing a measure of fault tolerance.
3) A neural network can analyze network data in a non-linear fashion. This characteristics is especially important in a networked environment where the information which is received is subject to the random failings of the system, and also because some attacks may be conducted against the network in a coordinated assault by multiple attackers. In a linear system, changing a single input produces change in the output, and the input's effect depends only on its own value. In nonlinear system, the effect depends on the values of other inputs and the relationship is a higher-order function. Systems in the real world are often nonlinear.
4) Speed – The high processing speed of the neural networks enable timely identification of attacks or instances of attacks against the system before irreparable damage occurs to the system. A neural network-based misuse detection system would identify the probability that a particular event, or series of events, was indicative of an attack against the system. Information regarding the occurrence of the event(s) indicating an attack can then be used to determine intrusion attempts for the purpose of conducting defensive measures before the attack is successful.
5) Neural networks can work in real time, online or batch modes in a highly parallel fashion. Their numerous identical independent operations can be executed simultaneously. Special hardware devices are being designed and manufactured which take advantage of this capability.

6) The arithmetic characteristics of ANN make ANN good at handling large volumes of data. ANN put more focus on the pattern identification rather than data analysis.
7) Fault tolerance via redundant information coding - Partial destruction of a network leads to corresponding degradation of performance. However, some network capabilities may be retained even with major network damage.

Notwithstanding their success, neural nets have a number of limitations which restrict their utilization in the detection of instances of misuse. These include:

1) The training and processing times of neural networks can be a very slow process when applying them to databases of realistic size or complex highly non-linear data. Input signals from large databases or event sets normally contain too much irrelevant information for event classification. The signals form complex patterns that cannot be easily broken down into a series of sub-problems which have an identifiable number of solutions.
2) The training routine requires a very large amount of sensitive data (individual attacks sequences) to ensure that the results are statistically accurate. These data training sets are difficult to acquire.
3) It is very difficult to understand why a neural network produces a score it did unlike most other methods. This "black box" nature of neural nets makes them adapt their analysis in response to the training which is conducted on the network. The connection weights and transfer functions of the various network nodes are usually frozen after the network has achieved an acceptable level of success in the identification of events. While the network analysis is achieving a sufficient probability of success, the basis for this level of accuracy is not often known, and this has plagued neural networks in a number of applications.

## MATERIALS

The process of ANN comprises three stages such as training, testing and deployment. In the training process, different weights are assigned nodes and layers by different training algorithms using the past data. The training of involves an iterative process where individual connection weights between synapses are repeatedly adjusted until the system converges to produce a derived output. The signals are changed when they travel along the connections: They are combined – usually by multiplication – with the connection weights. A neuron (Fig. 1) gathers the input from all incoming connections to compute its activation value.

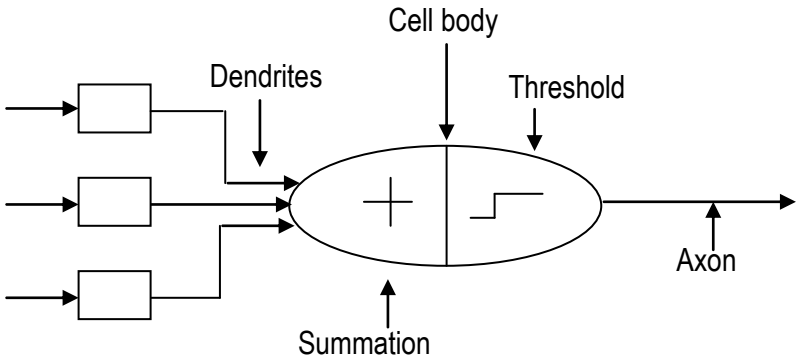




Fig. 1 The Neuron Model

In 1949, Hebb hypothesized about learning in networks of artificial neurons. The Hebb rule encodes the correlations of activations of connected units in the weights. A weight is increased if the two neurons that are connected by it are active at the same time. The weight is decreased if only one of the two connected neurons is active. The structure of an artificial neural network is illustrated in figure 2.

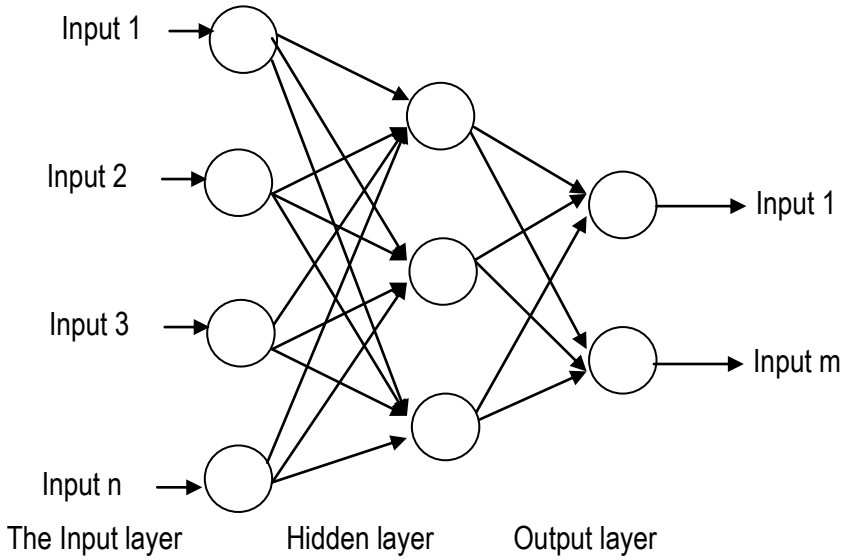


Fig. 2 The Structure of an Artificial Neural Network

Each hidden node performs a calculation on the signals reaching it and sends a corresponding output signal to other nodes. The final output is a highly processed version of the input.

| | | | | |
|---|---|---|---|---|
| Input to a Receivin element | = | Output of transmitting element | X | Weight of pathways linking element |

Three major learning paradigms are: supervised learning, unsupervised learning and reinforcement learning.

- **Supervised learning -** In the supervised training methods, both the input and the desired result are provided. And the output is compared with the desired data until the predetermined accuracy is obtained by changing different links and weights assigned to ANN.
- **Unsupervised learning -** Unsupervised learning is a method of machine learning in which only input data are given and human users do not compare output data with the desired results. Here, a model is fit to observations. It is distinguished from supervised learning by the fact that it requires no historical training data to train the system (i.e., no *a priori* output). The neural net is autonomous and as such it can determine some properties about data and reflect these properties in an output. Unsupervised neural nets take into consideration not only the properties of individual

events but the event's relationship with other events and the event's relationship to predetermined concepts which characterize the event collection. A data set of input objects is gathered, and unsupervised learning then typically treats input objects as a set of random variables. A joint density model is then built for the data set.

- **Reinforcement learning -** In reinforcement learning, data $x$ is usually not given, but generated by an agent's interactions with the environment. At each point in time $t$, the agent performs an action $y_t$ and the environment generates an observation $x_t$ and an instantaneous cost $c_t$, according to some (usually unknown) dynamics. The aim is to discover a *policy* for selecting actions that minimizes some measure of a long-term cost, i.e. the expected cumulative cost. The environment's dynamics and the long-term cost for each policy are usually unknown, but can be estimated.
- **Competitive learning -** Here, training data, consisting of input and desired output pairs are not available, but where the only information is provided by a set of input patterns $x^p$. In these cases the relevant information has to be found within the (redundant) training samples $x^p$.

## METHODS

There are two general implementations of neural networks in misuse detection systems. The first involves incorporating them into existing or modified expert systems. This proposal involves using the neural network to filter the incoming data for suspicious events which may be indicative of misuse and forward these events to the expert system. This configuration should improve the effectiveness of the detection system by reducing the false alarm rate of the expert system. Because the neural network will determine a probability that a particular event is indicative of an attack, a threshold can be established where the event is forwarded to the expert system for additional analysis. Since the expert system is only receiving data on events which are viewed as suspicious, the sensitivity of the expert system can be increased, (typically, the sensitivity of expert systems must be kept low to reduce the incidence of false alarms). This configuration would be beneficial to organizations that have invested in rule-based expert system technology by improving the effectiveness of the system while it preserves the investment that has been made in existing intrusion detection systems. The disadvantage of this approach would be that as the neural network improved its ability to identify new attacks the expert system would have to be updated to also recognize these as threats. If the expert system were not updated then the new attacks identified by the neural network would increasingly be ignored by the expert system because its rule-base would not be capable of recognizing the new threat.

The second approach would involve the neural network as a standalone misuse detection system. In this configuration, the neural network would receive data from the network stream and analyze the information for instances of misuse. Instances which are identified as indicative of attack would be forwarded to a security administrator or used by an automated intrusion response system. This approach would offer the benefit of speed over the previous approach, since there would only be a single layer of analysis. In addition, this configuration should improve in effectiveness over time as the network learns the characteristics of

attacks. Unlike the first approach, this concept would not be limited by the analytical ability of the expert system, and as a result, it would be able to expand beyond the limits of the expert system's rule-base.[1]

In this paper, the self-organizing feature map architecture which uses a single layer of neurons to represent knowledge from a particular domain in the form of a geometrically organized feature map is selected for this purpose.[4] The steps of the ANN model design is illustrated in the pseudo-code below:

1. ANN Model development
2. Software Implementation of ANN Model
3. Train the ANN model and test with a known data set
4. Deploy the ANN model and test with other known data sets
5. Compare ANN Model results with reality
6. Results ok?
   6.1 If No, fine-tune the ANN Model behaviour
   6.2 Go back to step 2
7. Deploy ANN permanently
8. End

## RESULTS AND DISCUSSION

The proposed Fraud Detection system aims to facilitate real-time transaction entry and react to a suspicious cooperation or transaction that may lead to fraud. Consequently, the design of the architecture is based on the following conditions:

i. The system runs secretly beneath the application software within identified network used for fraudulent transactions.
ii. Each new transaction entering the database is treated as a signature, suspected and prone for verification.
iii. Neural network agents are applied to the transactions data to generate two models or clusters: fraud and non-fraud cases.
iv. Business rules relevant to enlisted transactions are further applied to the two cases to detect transactions that deviate from the norms. Deviation from the usual pattern of any entity may imply the existence of a fraud. The overhead threshold, for obvious reasons, is a closely guarded secret and varies over time.
v. The similarity between a customer's current transaction and a known fraud scenario indicates the same fraud may occur again.
vi. Suspect's transactions are flagged within seconds, for further investigations and subsequent decisions making.
vii. Visualization is provided using appropriate GUI

The implemented architecture as illustrated in Fig.3 below consists of two subsystems: Database interface and Fraud detection engine.

1. The database interface subsystem is actually the entry point through which new transaction finds way into the system. It is system's interface with the application software.

2. Fraud detection subsystem: Each transaction entering into the system is passed to the host server where the corresponding transaction profile is further checked using multi-agents and transactions business rules relevant to an enlisted transaction that deviate from the norms.

3. The input Database Interface

The input database interface provides a graphical user-friendly interface with possibility of importing necessary business transaction data from the database. It enables the user to decide which transaction to check and facilitates selection of the transaction table/data for analysis.

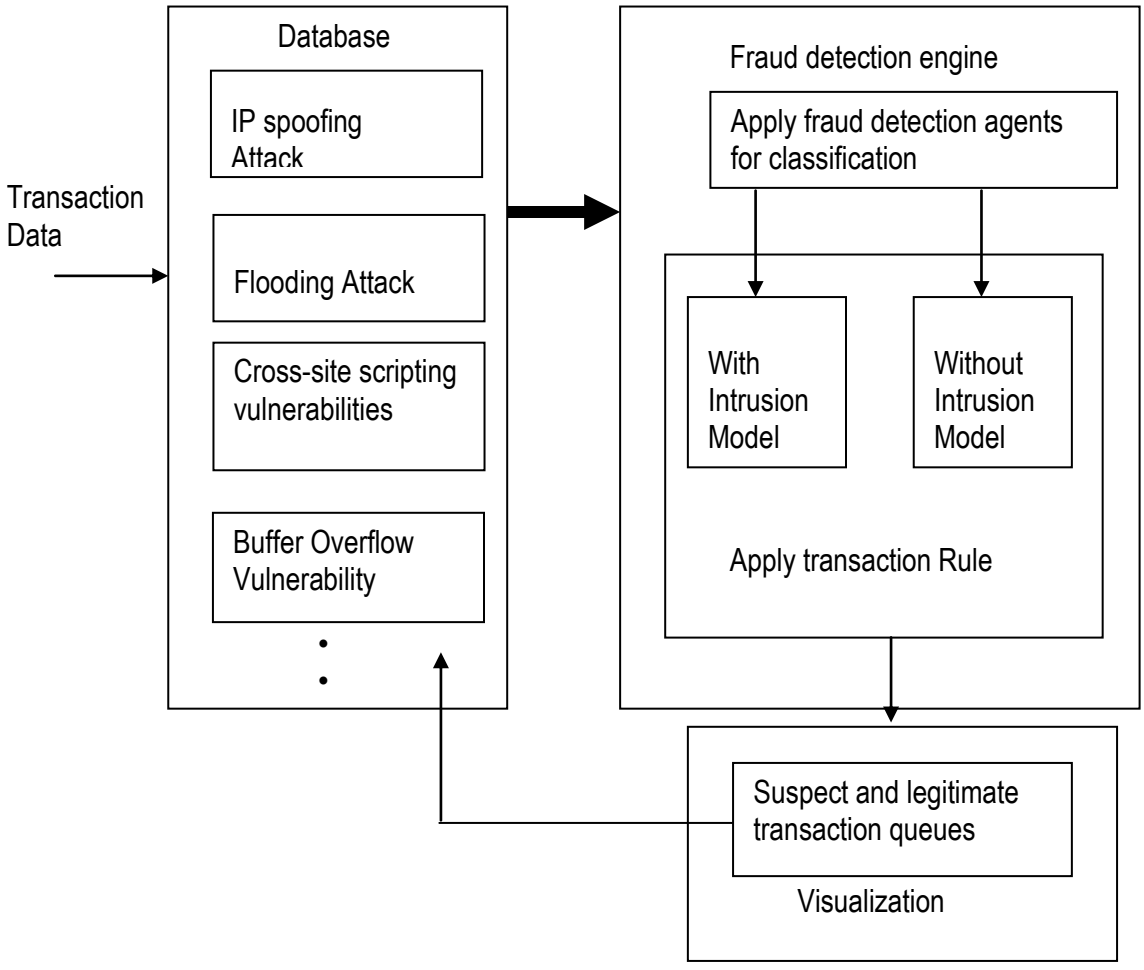


Fig 3 Architecture of the ANN-based Fraud Detection System

## CONCLUSION

Fraud detection is a particularly difficult problem because of the extensive number of vulnerabilities in computer systems and the creativity of the attackers. This paper have shown that a neural network-based fraud detection system provide the potential to identify and classify network activity based on limited, incomplete, and nonlinear data sources. It is clear that efficient, dynamic and adaptive fraud detection techniques will give service operators a competitive edge in terms of customer care and retention, marketing and revenue assurance.[3] ANN agent is one type of intelligent agent that can be deployed in a multi-agent architecture to distribute the solution to fraud detection so that it may be more of a real-time solution that is effectively managed.[4] This paper went further to propose mathematical models and algorithms as a possible solution.

The advantages of ANN were identified: they are adaptive, can generalize, are non-linear like all real-world systems meaning output depends on the values of other inputs, can handle large volume of data, and can retrain network capabilities in the face of faults. However, ANNs can be slow when the size of the training data sets and variables increases in complex application areas owing to difficulty in event classification of too many irrelevant and redundant information. Data training sets are also difficult to acquire and the outputs/results of ANNs can be very difficult to understand.

## REFERENCES

James Cannady. Artificial Neural Networks for Misuse Detection. School of Computer and Information Sciences, Nova Southeastern University, Fort Lauderdale, FL 33314, cannadyj@scis.nova.edu

Michiaki Taniguchi, Michael Haft, Jaakko Hollmén, and Volker Tresp. Fraud Detection in Communications Networks Using Neural and Probabilistic Methods. Siemens AG, Corporate Technology, Department Information and Communications, D-81730 Munich, Germany, (e-mail: Michiaki, Taniguchi@mchp.siemens.de).

Ikechukwu F. C. Onah, H. C. Inyiama, *2010.* Perception of Communication Network Fraud Dynamics by Network Administrators and Stake Holders. Ph.D research paper, Department of Computer Science, Ebonyi State University, Abakaliki, Nigeria.

Ikechukwu F. C. Onah, *2010.* A Self-Organizing Map Model for Network Fraud Pattern Classification. Ph.D research paper, Department of Computer Science, Ebonyi State University, Abakaliki, Nigeria.