IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 1, No. 3, September 2012, pp. 121~126
ISSN: 2252-8938

Multi-Party Security with SEP using Artificial Neural Networks

Urvashi Rahul Saxena*, S.P Singh**
* Department of Computer Science and Engineering, JSS Academy of Technical Education, Noida, India
** Department of Computer Science, Birla Institute of Technology, Noida, India

Article Info

Article history:

Received Jul 3, 2012
Revised Jul 26, 2012
Accepted Aug 5, 2012

Keyword:

Artificial Neural Network
Multi-Party Secured System
Network Security System
User Behavior Model
Intrusion Detection System.

ABSTRACT

Multi-Party Security System is an improvised version of various security systems available using Artificial Neural Networks (ANN's) as an Intelligent Agent for Intrusion Detection. This Paper focuses how inputs can be preserved to serve as a measure for securing communication protocol between two parties using privacy protocols at the hidden layer of Multi-layer Perceptron model. Various neural network structures are observed for evaluating the optimal network considering the number of hidden layers. Results depict that the generated system is capable of classifying records with about 90% of accuracy when two hidden layers are engulfed and the accuracy reduces to 87% with one hidden layer under observation.

Corresponding Author:

Urvashi Rahul Saxena
Departement of Computer Science and Engineering,
JSS Aademy of Technical Education,Noida, India
B-42, Kendriya Vihar, Sector-51, Noida, India-201301.
Email: urvashirahulsaxena@gmail.com

1. INTRODUCTION

In the last decades work on information technologies based on the computer networks played an important role in various spheres of human activity. Several problems trusted on them, such as keeping, transmission and automation of information processing. The security level of processed information can vary from private and commercial to military and state secret. Herewith the violation of the information confidentiality, integrity and accessibility may cause the damage to its owner and have significant undesirable consequences. Thus the problem of information security is concerned. Many organizations and companies develop security facilities that require significant contributions. On the other hand, the impossibility of creating completely protected system is a well-known fact – it will always contain mistakes and «holes» in its realization. To protect computer systems such accustomed mechanisms as identification and authentication, mechanisms of the delimitation and restriction of the access to information and cryptographic methods are applied.

However they possess following drawbacks:

- Exposure from internal users with malicious purposes;
- Difficulties in access differentiation caused by information resources globalization, which washes away differences between "own" and "foreign" subjects of the system;
- Reduced productivity and difficulty in communication due to mechanisms for access control to the resources, for instance, in e-commerce;
- Password definition by making association of simple users is simplified.

Thus, logging and audit systems are used along with these mechanisms; one amongst them is Intrusion Detection System (IDS).

This paper is described in various sections: Section II gives on overview of IDS (intrusion Detection System), Section III explains role of ANN in security, Proposal of SEP *(Secure Evaluation Protocol*) and

Simulation of SEP with Back-Propagation Algorithm; finally some conclusions are drawn from the proposed system.

2. INTRUSION DETECTION SYSTEM

IDS are usually divided to systems detecting already known attacks (*misuse detection systems*) and *anomaly detection systems* registering the life cycle deviations of the computer system from its normal (typical) activity. Intrusion Detection System (IDS) is an emerging new technology, being informed is the best weapon in the security analyst's arsenal. "An ounce of prevention is worth a pound of detection". An Intrusion Detection System detects attacks as soon as possible and takes appropriate action. Security is a compulsory need for data operation today. Information or commerce exchanges need security and reliability. Examples are like: Banking sector transactions where the need for financial security is mandatory, Protection of Personal Resources etc. Password based security system should possess facilities like:

- Provision to assign complex password without any restriction.
- Password must be encrypted up to proper level before storing or transmitting.
- Password reset procedure must be simplified.
- Facility to record and monitor failed login attempts.

Main drawbacks of the described IDS are:

- High probability ambiguous warnings;
- Prominent methods of determining new, unknown in advance intrusions;
- Unstable reaction to distributed attacks;
- Need of human expertise during all the working time.

To eliminate such defects new approaches were developed. They allow building completely or highly automated IDS [1]. These approaches are mainly directed on "intellectualization" of IDS. Among them two basic approaches are:

1. Use of neural networks [2-3], with the help of anonymization method using anonypro protocol [10].
2. Systems based on agent approach.

It is known, that approximately 70% of attacks are initiated from the inside of network. It might be as password stealing, so using vulnerabilities of information security and the software. Thus, modern approaches actively implement the user behavior model. Developing IDS it is also necessary to take into account distributed nature of attacks on computer network. All these factors show agents approach to be more preferred for creating the security systems.

3. ROLE OF ANN

The soft computing techniques have the ability of dealing with uncertain and partially true data makes them attractive to be applied in intrusion detection. Some studies have used soft computing techniques other than ANNs in intrusion detection. For example, genetic algorithms have been used along with decision trees to automatically generate rules for classifying network connections. ANNs are the most commonly used soft computing technique in IDSs.

An ANN is an information processing system that is inspired by the way biological nervous systems, such as the brain, process information. It is composed of a large number of interconnected processing elements (neurons) working with each other to solve specific problems. Each processing element (neuron) is basically a summing element followed by an activation function. The output of each neuron (after applying the weight parameter associated with the connection) is fed as the input to all of the neurons in the next layer. The process of learning is essentially an optimization process in which the parameters of the best set of connection coefficients (weighs) for solving a problem are found and includes the following basic steps:

- Present the neural network with a number of inputs
  (Vectors each representing a pattern)
- Check how closely the actual output generated for a
  A specific input matches the desired output and changes the neural network parameters (weights) to better approximate the outputs.

Some designers of IDS exploit the ANN as a pattern recognition technique. This technique of pattern recognition can be implemented by using a feed-forward neural network that needs to be trained accordingly.

Figure 1 Depicts feed-forward Neural Network. ANNs are usually initialized with random connection weights then adjust the weights a supervised learning algorithm called back-propagation. The algorithm works by presenting the network with a set of pre-classified training data. For each piece of data,

the inputs are fed forward through the network using the current connection weights. The back-propagation algorithm then examines the output values and compares them to the expected output for this piece of data. The error in the output value is sent backwards through the network, adjusting each connection weight a small amount. This small amount is the expected value subtracted from the actual value multiplied by a small learning rate constant. Typically each item in the training set is sent through the network several times to improve the accuracy. After enough iteration, the weights will stabilize on a set of values [6].

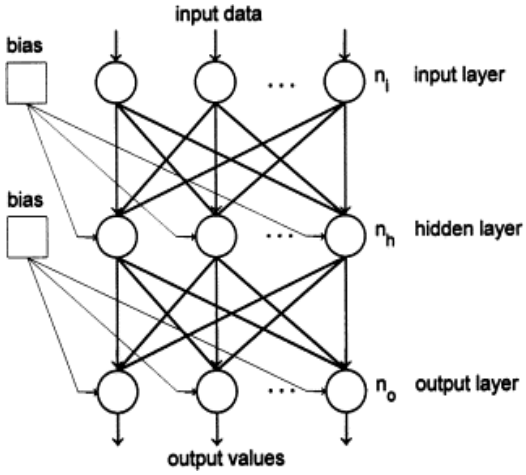

Figure 1. Feed-forward Neural Network

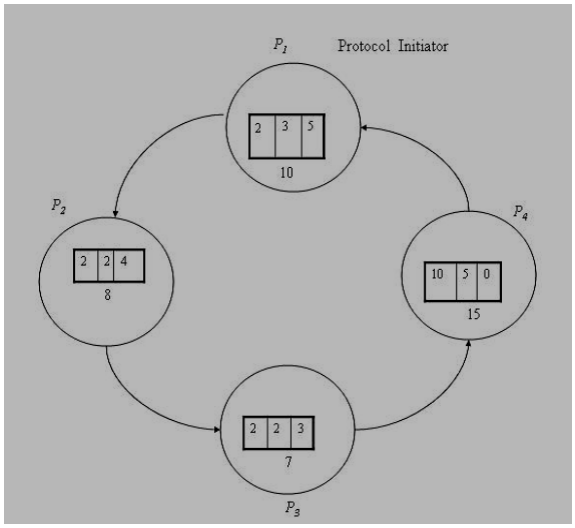

Figure 2 Initial architecture of *Secure Evaluation Protocol*

3.1. Multi-Party Security & ANN

This paper introduces S*ecure Evaluation Protocol* to ensure security by applying annonamization techniques to the inputs and securing them. Annonamization is a technique to hide the inputs to ensure the integrity of the output.The secure evaluation protocol proposed in [4] used random numbers for privacy of individual data inputs. In this scheme any two parties *Pi-1* and *Pi+1* can collude to know the secret data of party *Pi* by performing only one computation. Emphasis is laid in such a manner that the probability of data leakage is significantly reduced by breaking the data block of individual party in number of segments. The probability of data leakage decreases as the number of segments in a data block is increased. Thus, finally we will be able to come to a conclusion that more the number of hidden layers, lesser will be the data leakage. As per our survey no secure evaluation protocol is available in the literature with zero probability of data leakage when two neighbors collude. In this paper we proposed zero probability protocol for secure evaluation computation namely *ck-Secure Evaluation Protocol* in which neighbors are changed in each round of computation [7-9].

3.1.1 Proposed Architecture and Protocol Description

The initial architecture of the protocol is shown in Figure 2 where parties are arranged in a ring. Each party breaks the data block into *k* segments which is equal to *n*-1. For example in fig 2 four parties break their data block into three segments. Initially the parties are arranged sequentially as $P_1, P_2 ... P_n$. In the next round of the computation P_2 exchanges its position with P_3 and in subsequent rounds P_2 exchanges its position with P_4 and so on until P_n is reached [10].

Artificial Neural Network encapsulates *inputs* as the communicating parties, so by using the nearest neighbor approach each time a set of training pair is submitted to the ANFIS(Adaptive Neuro-Fuzzy Inference System) editor the neighbors' are exchanged thereby giving false impression of their presence to the malicious attackers.

It has been seen through various research work already done in the field of Neural network's that once the programmer is able to hide the inputs ,half the task is done.

3.1.2 Back-Propagation Algorithm and Secure Evaluation Protocol

The motivation for *Secure Evaluation Protocol* is that we change the neighbors in each round of segment computation. Thus it is guaranteed that no two semi honest parties can learn all the data segments of a victim party. In this protocol also each party breaks the data.

We propose *P1* to be the protocol initiator. The position of the protocol initiator is kept fixed in each round of computation. For the first round of the computation parties are arranged in a serial fashion as *P1, P2… Pn.* The protocol initiator starts computation using k-secure evaluation protocol to get the computation of first segment of each party. Before second round of computation starts *P2* exchanges its position with *P3.* In next round of the computation *P2* exchanges its position with *P4* and so on until *P2* exchanges its position with *Pn*. Generalizing the method we can say that in *ith* round of the computation *P2* exchanges its position with *Pi+1* until *Pn* is reached. In each round of computation segments are added using k-secure sum protocol [11] and the partial sum is passed to the next party until all the segments are added and the sum is announced by the protocol initiator party [11].A suitable Activation Function normally a *Sigmoid* function is always used along with the *Bias* to maintain the variation in the weights of the inputs and the summation of inputs, which will be submitted to the further layers for computation.

Accuracy of the *Secure Evaluation Protocol* depends upon the fact that more the number of hidden layers will be present to transit the data, security will have its means and the Intruders will have a minimum or negligible chance for hacking the data belong to an Authorized party.

Snapshots for a four-party case are shown in Figure 3.

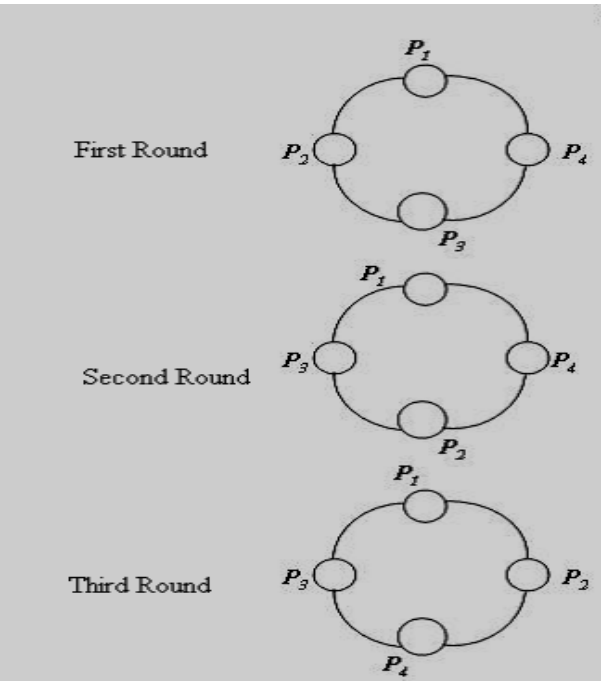

Figure 3. Snapshots for a four-party case

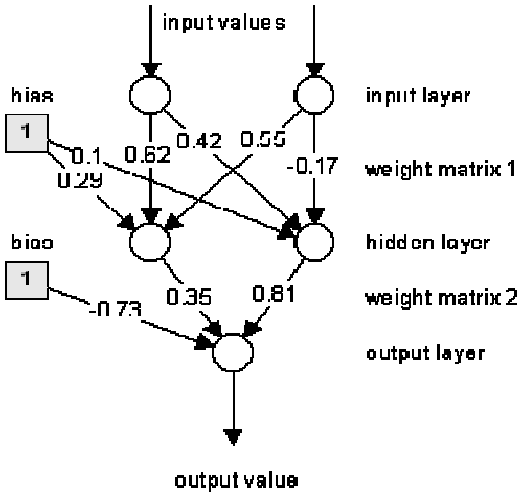

Figure 4 Layout of two hidden layers encapsulated by Secure Evaluation Protocol.

The algorithm: *Secure Evaluation*

1. Define $P_1, P_2, ..., P_n$ as inputs to the Neural Network behaving as *n communicating* parties where $n >= 4$.
2. Assume these parties have secret inputs $x_1, x_2 ... x_n$;
   Basically when we have two or more than two hidden layers Secure Evaluation Protocol is encapsulated in more appropriate manner as compared to a single hidden layer, since the concept of *changing neighbors* is portrayed better and yields more accurate result of computation.
3. Each node input (party) P_i breaks its data x_i into $k= n-1$ segments d_{i1} , d_{i2} ,…, d_{ik} such that $\Sigma\, d_{ij} = W_j x_i$ for $j = 1$ to k.
4. Arrange input parties in a ring as $P_1, P_2 ... P_n$ and select P_1 as the protocol initiator. (Simulation of Back Propagation Algorithm with Intrusion Detection System emphasizes that the while selecting any pair of input(s), small and random values must be taken into consideration, so that the Network does not saturates with high Input values, also as far as the maintenance of *momentum and Intensity(factors adjusting the Back-Propagation Algorithm)* of a Network based system is concerned, one must always initiate the system with smaller values so that the *Bias* i.e., the weight adjustment unit is able to manipulate and adjust the variations in the weights of the input units ranging from [-1 to +1]). Figure 4 represents such random and small values to explain SEP (Secure Evaluation Protocol) as:
5. Assume $rc = k$ and $S_{ij} = 0$. */* S_{ij} is partial evaluation and rc is round counter*/*

6. While *rc*!=0

```
Begin
        for j = 1 to k
        begin
             for i =1 to n
        begin
        starting from P1 each party computes cumulative
    sum Sij of the next layer; and the received sum
    from their neighboring layers and sends to the
    next input party in the ring encapsulating  layers
    of the feed-forward ANN.
    End;
       P2 exchanges its position with P(j+2) mod n
 End;
rc = rc – 1
End;
```

At each intermediate layer Bias value supported by the sigmoid activation function are used to generate accurate results [13]

7. Party P_1 announces the result as S_{ij} .
8. End of the Algorithm.

4. CONCLUSION

Secure Evaluation Computation is an important element of providing secured solutions using Artificial Neural Networks. SEP Protocols are needed for secure evaluation computation with greater security to individual data. The *Secure Evaluation Protocol* changes neighbors in each round of computation in the feed-forward neural network. Our proposed protocol provides zero probability of data leakage by two colliding parties when they want to attack data of a middle party defined as submitting a set of input patterns to be trained in the Back-Propagation Algorithm. This is an appreciable improvement over previous protocols available in the literature. Thus by submitting small and random values as a set of input pair for training we observe that with two hidden layers we are able to provide more secured service rather than with presence of a single hidden layer as more number of hidden layers enables the changing between neighbors efficiently. Efforts can be made to reduce the computation and the communication complexity preserving the property of zero hacking.

REFERENCES

[1] V.Gorodetski, O.Karsaev, A.Khabalov, I.Kotenko, L.Popyack, V.Skormin. Agent-based model of Computer Network Security System: A Case Study. Proceedings of the International Workshop "Mathematical Methods, Models and Architectures for Computer Network Security". Lecture Notes in Computer Science, vol. 2052, Springer Verlag, 2001, pp.39-50.

[2] James Cannady, James Mahaffey. The Application of Artificial Neural Networks to Misuse Detection: Initial Results.

[3] A.M. Reznik, N.N. Kussul, A.M. Sokolov. Neural network identification of the behavior of the users of computer systems. Cybernetics and computational techniques, 1999, vol.123, pages 70-79.

[4] C. Clifton, M. Kantarcioglu, J.Vaidya, X. Lin, and M. Y. Zhu, "Tools for Privacy-Preserving Distributed Data Mining,"*J. SIGKDD Explorations, Newsletter, vol.4, no.2, ACM Press,* pages 28-34, Dec. 2002.

[5] R. Sheikh, B. Kumar and D. K. Mishra, "Privacy-Preserving k-Secure Sum Protocol," in *International Journal of Computer Science and Information Security, vol. 6 no.2*, pages 184-188, Nov. 2009.

[6] R. Agrawal and R. Srikant. "Privacy-Preserving Data Mining," In *proceedings of the 2000 ACM SIGMOD on management of data*, Dallas, TX USA, pages 439-450, May 15-18 2000.

[7] M. J. Atallah and W. Du. "Secure Multiparty Computational Geometry," *In proceedings of Seventh International Workshop on Algorithms and Data Structures(WADS2001)*. Providence, Rhode Island, USA, pages 165-179, Aug. 8-10 2001.

[8] W. Du and M.J. Atallah. "Privacy-Preserving Cooperative Scientific Computations," *In 14th IEEE Computer Security Foundations Workshop*, Nova Scotia, Canada, pages 273-282, Jun. 11-13 2001.

[9] W. Du and M.J.Atallah, "Privacy-Preserving Statistical Analysis," *In proceedings of the 17th Annual Computer Security Applications Conference*, New Orleans, Louisiana, USA, pages 102-110, Dec. 10-14 2001.

[10] W. Du and M.J. Atallah, "Secure Multiparty Computation Problems and Their Applications: A Review and Open Problems," In *proceedings of new security paradigm workshop*, Cloudcroft, New Maxico, USA, pages 11-20, Sep. 11-13 2001.

[11] V. Oleshchuk, and V. Zadorozhny, "Secure Multi-Party Computations and Privacy Preservation:Results and Open Problems," *Telektronikk: Telenor's Journal of Technology, vol. 103, no.2*, 2007.

[12] D. K. Mishra, M. Chandwani, "Extended Protocol for Secure Multiparty Computation using Ambiguous Identity," *WSEAS.*

[13] A.C.Yao, "protocol for secure computations," in *proceedings of the 23rd annual IEEE symposium on foundation of computer science*, pages 160-164, Nov.1982.