Neural networks in intrusion detection systems

Neuronové sítě v systémech pro detekci napadení

A. VESELÝ, D. BRECHLEROVÁ

Czech University of Agriculture, Prague, Czech Republic

Abstract: Security of an information system is its very important property, especially today, when computers are interconnected via internet. Because no system can be absolutely secure, the timely and accurate detection of intrusions is necessary. For this purpose, Intrusion Detection Systems (IDS) were designed. There are two basic models of IDS: misuse IDS and anomaly IDS. Misuse systems detect intrusions by looking for activity that corresponds to the known signatures of intrusions or vulnerabilities. Anomaly systems detect intrusions by searching for an abnormal system activity. Most IDS commercial tools are misuse systems with rule-based expert system structure. However, these techniques are less successful when attack characteristics vary from built-in signatures. Artificial neural networks offer the potential to resolve these problems. As far as anomaly systems are concerned, it is very difficult to build them, because it is difficult to define the normal and abnormal behaviour of a system. Also for building anomaly system, neural networks can be used, because they can learn to discriminate the normal and abnormal behaviour of a system from examples. Therefore, they offer a promising technique for building anomaly systems. This paper presents an overview of the applicability of neural networks in building intrusion systems and discusses advantages and drawbacks of neural network technology.

Key words: Intrusion Detection System (IDS), misuse IDS, anomaly IDS, Kohonen´s self-organizing maps, backpropagation neural networks

Abstrakt: Bezpečnost informačního systému je jeho velmi důležitou vlastností a to zvláště dnes, kdy počítače jsou navzájem propojeny prostřednictvím internetu. Protože žádný systém nemůže být absolutně bezpečný, včasná a přesná detekce napadení je nezbytná. Proto byly navrženy Systémy detekce napadení (IDS). Jsou dva základní druhy IDS: misuse IDS a anomaly IDS. Misuse IDS systémy detekují napadení vyhledáváním charakteristického vzorce aktivity (signature), který odpovídá známým typům napadení. Anomaly IDS systémy detekují napadení sledováním činnosti systému a zjišťováním, zda jeho chování nevybočuje z normálu. Většina komerčních produktů jsou misuse IDS se strukturou expertního systému řízeného pravidly. Tato technika je však méně úspěšná v případě, kdy vzorec aktivity při aktuálním napadení se odlišuje od charakteristického vzorce, který byl zabudován do systému. Umělé neuronové sítě nabízejí způsob, jak tento problém řešit. Anomaly IDS systémy je velmi těžké navrhovat, protože je těžké definovat normální a abnormální chování systému. Také zde mohou být s výhodou použity neuronové sítě, protože se mohou naučit rozlišovat normální a nenormální chování systému na základě předložených příkladů. V tomto článku je podán přehled možností aplikace neuronových sítí při vytváření systémů detekce napadení a jsou diskutovány výhody a nevýhody jejich použití.

Klíčová slova: systém detekce napadení (IDS), misuse IDS, anomaly IDS, Kohonenovy samoorganizující se mapy, neuronové sítě se zpětným šířením chyby

INTRODUCTION

Today, when computers are interconnected via internet and information systems gather and store important data, security of an information system is its crucial property. A secure information system should provide: data confidentiality, data and communications integrity and assurance against the denial-of-service (Mukherjee 1994). Data confidentiality protects data against an unauthorized disclosure. Data integrity is concerned with the accuracy, faithfulness and noncorruptibility of data. Denial of service is a threat, which takes place whenever the quality of system services falls below a predefined threshold or if the system services are completely inaccessible.

The conventional approach to secure information system is to build a protective shield around it. For this purpose, different methods of identification, authentication and mandatory access control techniques are used. But there is a number of limitations to this prevention based approach. First, it is probably impossible to build a system, which is completely secure. Futher, it could be impractical: the prevention based security philosophy necessarily constrains the user's activity and productivity (Ilgun 1995).

The contibution presented at the international conference Agrarian Perspectives XII (CUA Prague, September 18–19, 2003).

In the late 80ies, an alternative approach to the system security, called intrusion detection, was taken. The goal of the intrusion detection system is to identify activities that violate an organization security policy. Intrusion detection system is all the time supervising the information system and in the case of its intrusion, it sends warning or initiates certain defence actions.

Intrusion detection systems (IDS) can be classified into two main categories: misuse and anomaly intrusion detection systems. Misuse refers to the known attacks that make use of the known system vulnerabilities. Misuse systems define attack signatures, i.e. patterns of activity that are known to be undesirable. Then misuse systems are monitoring the system activity in order to find out the defined signatures, the presence of which indicates an attack. Each misuse system has several draw-backs. First, it is difficult to create an exhaustive attack database and so some attacks might be unrecognised. Furthermore, a small variation of a known attack might differ from the predefined signature put into database and the misuse system can miss the attack event entirely.

Anomaly systems are based on a different principle. They define a model of acceptable system activity and try to identify the behaviour that differs from this model.

There are two important characteristics of an intrusion system: false positive error rate and false negative error rate. False positive error rate counts false alarms and false negative error rate counts missed intrusions. Misuse systems are inclined to have a big false negative error rate and a small false positive error rate. Anomaly systems, on the contrary, are inclined to have a big false positive error rate and a small false negative error rate.

Technical realization of misuse systems is usually easier in comparison with the technical realization of anomaly systems. It is based on expert knowledge of the usual attacks. From this knowledge, a database of attack signatures is built up. Anomaly systems are more difficult to realize because it is difficult to explicitly define the normal behaviour of a system. Using neural networks, which can learn the normal behaviour of the system from examples, it is possible to facilitate their realization.

NEURAL NETWORKS

Artificial neural networks are a computing technology, which was conceived at the beginning of the 40ies of the last century and then developed in the region of artificial intelligence. Nowdays, it is considered to be a part of soft computing.

In the intrusion detection systems, the following two kinds of neural networks are used:
– multilayered feedforward neural networks
– Kohonen's self-organizing maps.

MULTILAYERED FEEDFORWARD NEURAL NETWORKS

Multilayered feedforward neural networks (ANNs) are in essence non-parametric regression methods, which approximate the underlying functionality in data by minimizing the loss function. The common loss function used for training an ANN is a quadratic error function. ANNs use supervised learning for adaptation. The database forms a training set. During the training, specified items of data records are put on the input of the neural network and its weights are changed in such a way, so that its output would approximate values in the data set. After finishing the learning process, the learned knowledge is represented by the values of neural network weights. For training, the algorithm of back propagation of error is often used. Back propagation of error algorithm was first introduced by Rumelhart (1988).

In Figure 1, there is an example of an ANN with 3 layers: input layer, output layer and hidden layer. It was proved, that one hidden layer is sufficient for the approximation of an arbitrary continual function.

ANNs could be used in many decision-making applications. Their advantages in these applications are:

– Capability of learning from examples.

– Capability of abstraction. It means that ANNs are able to efficiently decide also in situations which did not occur in the training set.

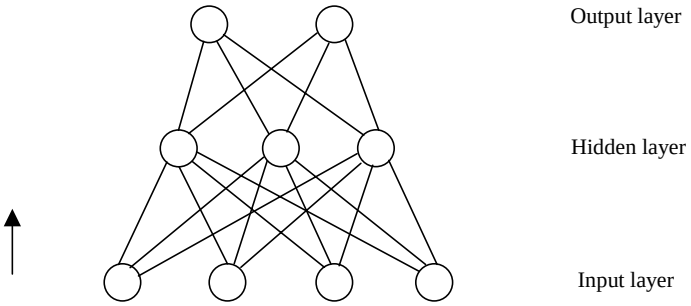

Figure 1. Multilayered feed-forward neural network (ANN)

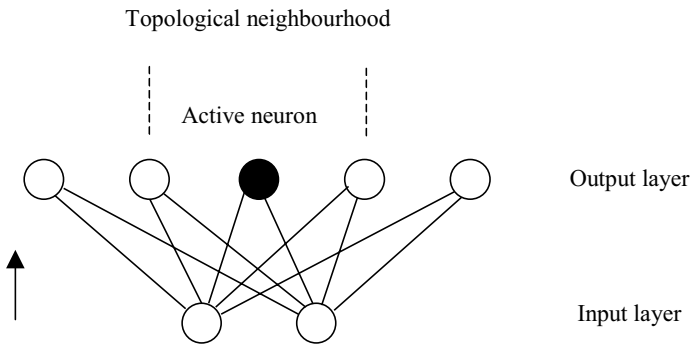

Figure 2. Kohonen' self-organizing map

KOHONEN'S SELF-ORGANIZING MAPS

Kohonen's self-organizing maps (SOMs) have become a promising technique in cluster analysis (Kohonen 1982). They are adapted by unsupervised learning.

The unsupervised learning process in SOM can be briefly described as follows (Figure 2). The connection weights are assigned with small random numbers at the beginning. The incoming input vectors presented by the sample data are received by the input neurons. The input vector is transmitted to the output neurons via the connections. In a "winner-take-all" competition, the output neurons with the weights most similar to the input vector became active. In the learning stage, the weights are updated following Kohonen's learning rule. The weight update only occurs for the active output neurons and its topological neighbours. The neighbourhood starts large and slowly decreases in size over time. Because the learning rate is reduced to zero, the learning process eventually converges.

After the learning process, similar sets of items activate the same neuron. SOM divides the input set into subsets of similar records. Therefore, SOM is a method of cluster analysis and is often used for vector quantization.

MISUSE IDS WITH NEURAL NETWORKS

Misuse systems are based on expert knowledge of the usual attacks. From this knowledge, a database of attack signatures is built up. The misuse system spends a lot of time doing a comparison of the system activity with a database of attack signatures. Some signatures are simple to define and the algorithm for the database check is straightforward. For example, when information system is running under the Unix operating system, one of the signatures could be the appearance of a new file with the root ownership and with enabled setuid bit. This signature is simply defined and could be simply tested.

Sometimes, a signature could not be defined easily. A typical example is a port scan. Port scan can be considered as an attempt to intrude the system, usually via internet. An intruder tries to find out a vulnerable server residing on some port. Although the intruder does not do any direct damage, one typically treats a port scan as an attack due to its possible malicious implications. Therefore, the misuse system should look for such events. The problem is to define a signature of this event. Misuse system has to analyse the incoming packets, which could be in some items modified by intruder to overcome revealing. A straightforward port scan is relatively easy to detect because of the same source address, source port address and because every destination port is eventually tried. However, the intruder can change the source address and source port in packets and send packets over a long time period, for example, by probing a single port every few hours.

In this situation, neural networks could be used (Cannady 1998). The principle of neural solution is described in Figure 3. Important items of the incoming packets $p_1, \ldots, p_n$ are chosen in the Feature extraction block. The output of the Feature extraction block $q_1, \ldots, q_n$ is then put at the input of SOM neural network. SOM classifies each input q_i into one of clusters, which it represents. To each neuron of SOM, i.e. to each cluster, there is beforehand assigned a number. Numbers assigned to the clusters into which the incoming packets were classified form a trace, which is then fed into the backpropagation network. Numbers assigned to SOM nodes have to be chosen in such a way, that the topology of SOM lattice was preserved. It means that numbers assigned to the nodes of SOM lattice, which are near neighbours, do not differr a lot. The sequence $p_1, \ldots, p_n$, which is fed into the system, consists of the last several hundred packets. The SOM block of the system must be trained beforehand by unsupervised learning and backpropagation network by supervised learning. In the similar way, a SYN flood attack could be detected. Also brute-force attacks on FTP server, when login attempts are dispersed overtime, could be detected by the above described neural network based system.

ANOMALY IDS WITH NEURAL NETWORKS

Anomaly detection systems do not know what the specific intrusions look like. They have the model of normal

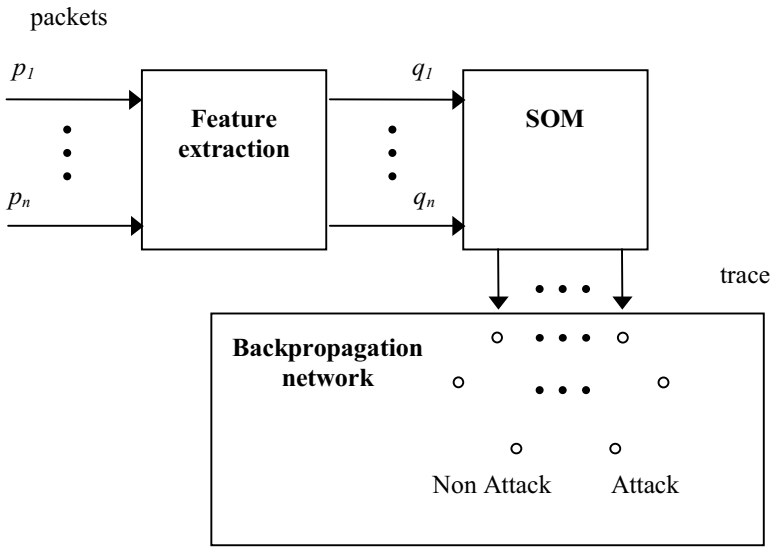

Figure 3. Neural part of misuse intrusion system

behaviour of the system and they look for deviations from the normal behaviour as potential intrusions.

The main difficulty in building up an anomaly system lays in defining normal behaviour of the system. To describe a normal behaviour of a system is usually possible only to a certain extent. For example, suppose that users log into the system every week after coming to work between 8 and 9 in the morning and log out when they leave between 4 and 6 in the afternoon. Suppose that the system finds out that between 1 and 2 a.m. most of users were logged into the system. This event is very abnormal and could be a sign of an unauthorized activity. By identifying this anomaly, anomaly system could identify a potential intrusion.

To define a normal activity of the system in general is a very difficult task. For this purpose, one can try to use neural networks and takes advantage of their ability to learn from examples and their capability of abstraction. The learning ability means that it is not necessary to define normal behaviour of the system explicitly. Generalization allows the anomaly system to recognize when an attack has been mutated slightly. The neural network should be able to recognize a variant of an attack that might be missed by a misuse system. Furthermore, generalization may allow the anomaly system to recognize conditions that are typical of an attack in general. If entirely new attacks exhibit these characteristics, the system may be able to identify them without ever having seen them before.

For example, NNID (Neural Network Intrusion Detector) (Ryan 1998) is a backpropagation neural network trained to identify users based on what commands they use during the day. The NNID system is implemented in the Unix environment. Unix is keeping for each user the log of commands which the user executed, together with values of consumption of the system resources per command. NNID takes into account the processor time used by the executed commands during one day. A vector called user profile thus characterizes each user. This is justifiable because different users tend to exhibit different behaviour, depending of their needs of the system. The set of commands used by a user and their consumption of processor time is therefore typical for each user and constitutes a ´print´ of this user. The system was tested for 100 commands and 10 users. Backpropagation network had 10 output neurons, i.e. one output neuron per user. When a user profile was put into input, the network was trained so that the output of corresponding neuron was 1 and outputs of the other neurons were 0. After training, the system could discriminate between user profiles and randomly generated profiles, which represented profiles of intruders. (When no output neuron had output value greater than 0.5, the profile was classified as a profile of an intruder.) The gained results were satisfactory. But unsolved questions remained: how well does the performance of NNID scale with the number of users and what would be behaviour of the system when users´ behaviour would change over time.

CONCLUSION

Research and development of intrusion detection systems have been under progress since 1980´s. Experiments during 1990´s have shown, that the neural network technology could provide useful means for solving difficult problems that designers of detection systems have to overcome. In misuse detection systems, the combination of SOM network and backpropagation neural network supply a very efficient means for detection of net intrusions as is for example Port scan. In the design of an anomaly detection system, one can take advantage of the neural network ability to learn and of its capability to generalize. Neural net can learn to discriminate between

normal and abnormal behaviour of the system from examples. No explicit definition of abnormal behaviour of the system is necessary and thus the main obstacle in building anomaly system could be overcome. Neural network approach is still in development, nevertheless it seems to be very promising for the future.

REFERENCES

Cannady J., Mahaffey J. (1998): The Application of Artificial Neural Networks to Misuse Detection, Georgia Tech Research Institute, http://www.raid-symposium.org/raid98/Talks.html# Cannady_34.

Denning D.E. (1987): An Intrusion Detection Model. IEEE Transaction on Software Engineering, SE-13: 222–232.

Ilgun K., Kemmerer R.A., Porras P.A. (1995): State Transition Analysis: A Rule-Based Intrusion Detection Approach. IEEE Transaction on Software Engineering, *21* (3): 181–199.

Kohonen T. (1990): The Self-organizing Map. Proceedings of the IEEE, *78* (9): 1464–1480.

Mukherjee B., Heberlein L.T., Levitt K.N. (1994): Network Intrusion Detection. IEEE Network: 26–41.

Rumelhart D.E. (1988): Parallel Distributed Processing. Vol. I and II, MIT Press, Cambridge.

Ryan J., Lin M.J., Mikkulainen, R. (1998): Intrusion Detection with Neural Networks. Advances in Neural Information Processing Systems, 10, MIT Press, Cambridge.

Arrived on 5th December 2003

Contact address:

Ing. Arnošt Veselý, CSc., RNDr. Dagmar Brechlerová, Česká zemědělská univerzita, Kamýcká 129, Praha 6-Suchdol, Česká republika
e-mail: vesely@pef.czu.cz, brechlerova@pef.czu.cz