Introduction of Soft Computing Systems for Software Security Management

Aslam Atiq, Dr R. S. D. Wahidabanu

Vinayaka Mission's Research Foundation University Salem, Tamil Nadu, INDIA
Mailing Address: Gulistan, M.A.Johar Road, Civil Lines, Rampur (U.P) 244901, INDIA
aslat@rediffmail.com

Abstract

Soft Computing is a general term for algorithms that learn from human knowledge and mimic human skills. We survey the principal constituents of soft computing techniques including Fuzzy Logic, Artificial Neural Networks, Support Vector Machines, Probabilistic Reasoning, Genetic Algorithms and Multi-Variate Adaptive Regressive Splines. Soft Computing techniques are being widely used by the IDS community due to their generalization capabilities that help in detecting known and unknown intrusions or the attacks that have no previously described patterns. Due to increasing incidents of cyber attacks, building effective intrusion detection systems (IDSs) are essential for protecting information systems security. This paper describes the use of soft computing techniques to detect the unknown intrusions and evidences that soft computing technique is better than previous used techniques to detect the intrusions.

Keywords: *Information technologies, Systems security, Intrusion detection, Intrusion detection system, Soft Computing evolution, Soft Computing types.*

1. Introduction

During last decades information technologies based on the computer networks play an important role in various spheres of human activity. Information has become the organizations most precious asset. Organizations have become increasingly dependent on the information since more information is being stored and processed on network-based systems. The widespread use of e-commerce has increased the necessity of protecting the system to a very high extent. Problems of great importance are entrusted 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 to many organizations and companies for development of security facilities that require significant contributions. 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. With the advent of soft computing, intrusion detection has become an integral part of the security process.

2. Intrusion Detection

Intrusion detection is defined as the process of intelligently monitoring the events occurring in a computer system or network, analyzing them for signs of violations of security policy. The primary aim of Intrusion Detection System (IDS) is to protect the availability, confidentiality and integrity of critical networked information systems. Intrusion Detection Systems are an important component of defensive measures protecting computer systems and networks from abuse. When an IDS is properly deployed it can provide warnings indicating that a system is under attack. It is critical for intrusion detection in order for the IDS to achieve maximal performance.

Intrusion Detection System are characterized based on two aspects

a) the data source (host based/ multiphase based/ network based;
b) the model of intrusion detection (anomaly detection/ misuse detection).

Intrusion detection attempts to detect computer attacks by examining data records observed by processes on the same network. These attacks are typically split into two categories, host-based attacks and network-based attacks. Host-based attack detection routines normally use system call data from an audit process that tracks all system calls made on behalf of each user on a particular machine. These audit processes usually run on each monitored machine. Network-based attack detection routines normally use system calls made on behalf of each user on a particular machine. These audit processes usually run on each monitored machine. Network-based attack detection routines typically use network traffic data from a Network sniffer (e.g. tcpdump). Many computer networks, including the widely accepted Ethernet (IEEE 802.3) network, use a shared medium for communication. In a misuse detection based IDS, intrusions are detected by looking for activities that correspond to known signatures of intrusions or vulnerabilities. On the other hand, an anomaly based IDS detects intrusions by searching for abnormal network traffic.

An intrusion detection system can be described at a very macroscopic level as a detector that processes information coming from the system to be protected. This detector can also launch probes to trigger the audit process, such as requesting version numbers for applications. It uses three kinds of information: long-term information related to the technique used to detect intrusions (a knowledge base of attacks for example), configuration information about the current state of the system, and audit information describing the events that are happening to the system. The role of the detector is to eliminate unneeded information from the audit trail. It then presents either a synthetic view of the security-related actions taken during normal usage of the system, or a synthetic view of the current security state of the system. A decision is then taken to evaluate the probability that these actions or this state can be considered as symptoms of an intrusion or vulnerabilities. A countermeasure component can then take corrective action to either prevent the actions from being executed or change the state of the system back to a secure state.

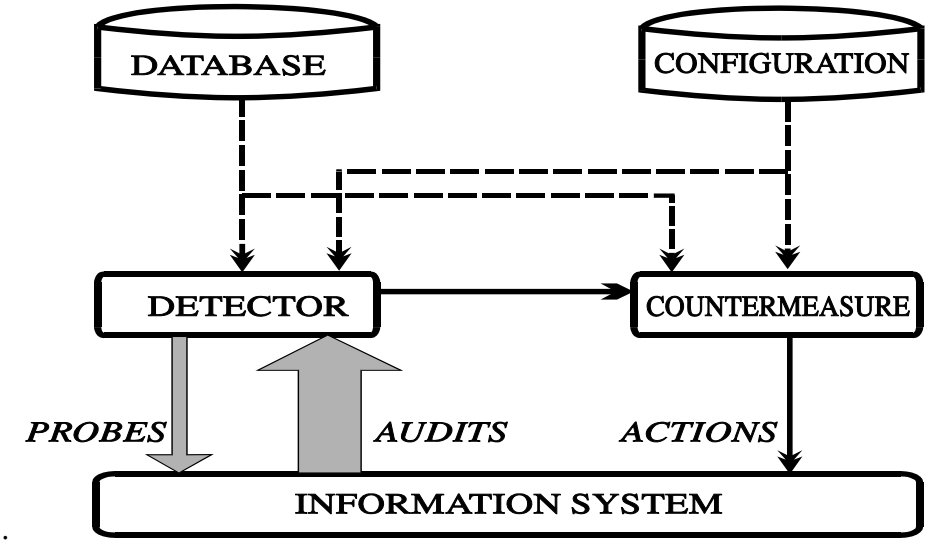

Fig 1. Intrusion – detection system

3. Evolution of Soft Computing

Soft Computing is a general term for optimization and processing techniques that are tolerant of imprecision and uncertainty. The idea behind the application of soft computing techniques and particularly Artificial Neural Networks in implementing IDSs is to include an intelligent system that is capable of disclosing the latent patterns in abnormal and normal connection audit records. The abnormal traffic pattern can be defined either as the violation of accepted thresholds of frequency of

events in a connection or as a user's violation of the legitimate profile developed for his/her normal behavior. One of the most commonly used approaches in expert system based intrusion detection systems is rule-based analysis using Denning's profile model. Rule-based analysis relies on sets of predefined rules that are provided by an administrator or created by the system. Unfortunately, expert systems require frequency updates to remain current. This design approach usually results in an inflexible detection system that is unable to detect an attack of the sequence of events is even slightly different from the predefined role. The problem may lie in the fact that the intruder is an intelligent and flexible agent while the rule based IDSs obey fixed rules. This problem can be tackled by the application of soft computing techniques in IDSs. Several artificial intelligence techniques have been utilized to automate the intrusion detection process to reduce human intervention, several such techniques include neural networks, fuzzy inference systems, evolutionary computation, machine learning and so on. The ability of soft computing techniques for dealing with uncertain and partially true data makes them attractive to be applied in intrusion detection. For example genetic algorithms have been used along with decision trees to automatically generate values for classifying network connections. However ANN's are the most commonly used soft computing technique in IDSs.

4. Artificial Neural Networks

Artificial Neural Networks are a form of connectionist learning, where knowledge is learned and remembered by a network of interconnected neurons, weighted synapses and threshold logic units. An ANN is an information processing system that is inspired by the way biological neuron systems, such as the brain, process information. It is composed of a large number of highly 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 learning process is essentially an optimization process in which the parameters of the best set of connection coefficients (weights) for solving a problem are found. Since ANNs are capable of making multi-class classifications, an ANN is employed to perform the intrusion detection.

5. Support Vector Machines (SVM)

Support Vector Machines have been proposed as a novel technique for intrusion detection, they are learning machines that place the training vectors in high-dimensional feature space labeling each vector by its class. SVMs are powerful tools for providing solutions to classification, regression, density estimation problems. These are developed on the principle structural risk minimization. Structural risk minimization seeks to find a hypothesis for which one can find the lowest probability of error. SVMs classify data by determining a set of vectors from the training set, called support vectors, which outlines a hyper plane in the feature space. The SVM approach transforms data into a feature space F that usually has a dimension. It is interesting to note that SVM generalization depends on the geometrical characteristics of the training data, not on the dimensions of the input space. Training a support vector machine (SVM) leads to a quadratic optimization problem with bound constraints and one linear equality constraint. There are other reasons we use SVMs for intrusion detection. The first is speed, as real time performance is of primary importance in IDSs any classifier that can potentially run "fast" is worth considering. The second reason is scalability: SVMs are relatively insensitive to the number of data points and the classification complexity does not depend on the dimensionality of the feature space, so they can potentially learn a larger set of patterns and thus be able to scale better than neural networks.

6. Fuzzy Logic

Fuzzy Logic introduced by Zadeh (1965) gives us a language, with syntax and local semantics, in which we can translate our qualitative knowledge about the problem to be solved. FLs main characteristic is the robustness of its interpolative reasoning mechanism. While Artificial Neural Networks require a "teacher" to provide data for the "learning", it mimics human or other "teacher" by repeating exactly what the "teacher" did in exactly the same situation. Fuzzy Logic emphasizes on rules that map situations to actions. It does not try to mimic exactly what the "teacher" does but aim at extracting the essence of decision making process of the "teacher". Fuzzy concepts derive from fuzzy phenomena that commonly occur in the natural world. For instance "rain" is a fuzzy statement of "Today raining heavily". Since there is no clear boundary between "rain" and "heavy rain". In intrusion detection suppose we want to write a rule as given below we need a reason about a quantity such as the number of different destination IP addresses in the last 2 seconds

IF the number of different destination addresses during the last n seconds was high

THEN an unusual situation exists.

6.1 Fuzzy Cognitive Maps

Fuzzy Cognitive Maps originated from the combination and synergism of fuzzy logic and neural networks combining the robust properties of both. Fuzzy Cognitive Maps provide an efficient soft computing tool that supports adaptive behavior based on empirical prior knowledge and provides a graphical representation of that knowledge that can be used for explanation of reasoning. The building blocks of neuro-fuzzy systems are non-linear functions such as the logistic function for many neuronetworks and generalized bell function for fuzzy controllers. These non-linear functions are applied to are combined by linear weighting mechanisms to achieve the required complex functional mapping which describes the control task at hand.

7. Genetic Algorithms

Genetic Algorithms were developed based on the principle of genetics using chromosomal operations such as crossover and mutation (Booker, Goldberg and Holland 1990; Goldberg 1989, Koza 1992). In these algorithms a population of individuals (potential solution) undergoes a sequence of unary (mutation) and higher order (crossover) transformation. After some number of generations the algorithm converges, the best individuals represent the desirable optimal solution. As genetic algorithms can be implemented at machine code level it will be fast to detect intrusions in a real-time mode. In the automatic induction of machine code by genetic programming, individuals are manipulated directly as binary code in memory and executed directly without passing as interpreter during fitness calculation. The LGP tournament selection procedure puts the lowest selection pressure on the individuals by allowing only two individuals to participate in the tournament. A copy of the winner replaces the loser of each tournament. The process of determining which items are most useful is called feature selection in the machine learning literature, genetic algorithms are used to select the measurements from the audit trail that are the best indicators for different classes of intrusions and to "time" the membership function for the fuzzy variables.

8. Probabilistic Reasoning Systems

The earliest probabilistic techniques are based on single-valued representations. The techniques started from approximate methods and evolved into formal methods for propagating values. In different approaches the basic inferential mechanism is the conditioning or updating operation. The two main currents within probabilistic reasoning are Bayesian Belief Networks and

Dampster-Shafer's theory of belief. In probabilistic reasoning knowledge is represented using the usual formalism of probability theory. Probabilistic Reasoning gives us the mechanism to evaluate the outcome of intrusion detection systems affected by randomness or other types of probabilistic reasoning.

9. Multi-Variate Adaptive Regression Splines (MARS)

Splines can be considered an innovative mathematical process for complicated curve drawings and function approximation. To develop a spline, the X-axis is broken into a convenient number of regions. The boundary between regions is also known as a knot. With a sufficiently large number of knots virtually any shape can be well approximated. While it is easy to draw a spline in two-dimension by keying on knot locations(approximating using linear, quadratic or cubic polynomial, etc.), manipulating the mathematics in higher dimensions is best accomplished using basis functions. In intrusion detection it will involve more computationally intensive goodness of fit measures, a generalized cross-validation procedure is used to determine the significant input features for intrusion detection, non-contributing input variables are thereby eliminated.

Comparison of Expert Systems, Fuzzy Systems, Neural Networks and Genetic Algorithms

	ES	*FS*	*NN*	*GA*
Knowledge representation	☑	☑	☐	■
Uncertainity tolerance	☑	☑	☑	☑
Imprecision tolerance	☐	☑	☑	☑
Adaptability	☐	■	☑	☑
Learning ability	☐	☐	☑	☑
Explanation ability	☑	☑	☐	■
Knowledge discovery and data mining	☐	■	☑	☑
Maintainability	☐	☑	☑	☑

* The terms used for grading are :
☐- bad, ■rather bad, ☑- rather good and, ☑- good

Table 1. Comparison of Different Algorithms

10. Conclusion

We have provided a brief survey of soft computing techniques in a variety of IDSs. With the increasing incidents of cyber attacks, building effective intrusion detection models with good accuracy and real-time performance are essential. This field is developing continuously. More hybrid soft computing techniques should be investigated and their efficiency evaluated as intrusion detection models.

References

[1] Abraham, A. and Jain, R. Soft Computing Models for Intrusion Detection Systems, Cryptography and Security ACM- class, 2004.

[2] Abraham, A. Grosan, C. and Chen, Y. Cyber Security and the Evolution of Intrusion Detection Systems, 2004.

[3] Bashah, N., Shannigan, I. B. and Ahmed, A. M. Intelligent Intrusion Detection System, Transactions on Engineering Computing and Technology V6, 2005.

[4] Benitez, J. M., Castro, J. L. and Requena, I. Are Artificial Neural Networks Black Boxes?, IEEE Trans on Neural Networks, 1996

[5] Bessiere, P. Genetic Algorithms Applied to Formal Neural Networks,1991.

[6] Bonissone, P. P. Soft Computing: the Convergence of Emerging Reasoning Technologies, Springer Verlag, 1997.

[7] Bwens, A., Palagiri, C., Smith, R., Szymanski, B. and Embrecht, M. Network Based Intrusion Detection Using Neural Networks, Proc. Artificial Neural Networks in Engineering, 2000, pp 489-494.

[8] Debar, H. An Introduction to Intrusion Detection Systems, IBM Research Zurich Research Lab, Saumerstrasse, 2000

[9] Kustn, I. and Thornton, C. Design of Artificial Neural Networks Using Genetic Algorithms: review and prospect.1994.

[10] Moradi, M. and Zulkernine, M. A Neural Network Based System for Intrusion Detection and Classification of Attacks, Springer Lecture Notes in Computer Science, 2006.

[11] Mukkamala, S. and Sung, A.H. Feature Selection for Intrusion Detection using Neural Networks and Support Vector Machines, Joournal of the Transportation Research Board, 2003.

[12] Mukkamala, S., Sung, A.H., and Abraham, A. Designing Intrusion Detection Systems: Architectures, Challenges and Perspectives, 2003.

[13] Mukkamala, S., Sung, A.H., and Abraham, A. Intrusion Detection Using Ensemble of Soft Computing Paradigms, Journal of Network and Computer Applications, Vol 28, Issue 2, 2005, pp 167-182.

[14] Mukkamala, S., Sung, A.H. and Abraham, A. Hybrid multi-agent framework for detection of stealthy probes, Applied Soft Computing, 2006.

[15] Negenvitsky, M. A Guide to Intelligent Systems, Addison Wesley, 2002.

[16] Schetmin, V. Learning from Web: Review of Approaches, Neural and Evolutionary Computing, 2005.

[17] Siraj, A., Bridges, S.M. and Vaughn, R. B. Fuzzy Cognitive Maps for Decision Support In an Intelligent Intrusion Detection System. Joint 9th IFSA World Congress and 20th NAFIPS International Conference, Vol 4, 2001, pp 2165-2170.

[18] Thomas, J. and Abraham, A. Distributed Intrusion Detection Systems: A Computational Intelligence Approach, Applications of Information Systems to Homeland Security and Defense, Chapter 15, 2005, pp 105-135.

[19] Wen, W., Callahan, J and Napolitano, M . Verifying Stability of Dynamic Soft Computing Systems, 1997.

Article received: 2008-02-21