

FUZZY COGNITIVE MAPS FOR DECISION SUPPORT IN AN INTELLIGENT INTRUSION DETECTION SYSTEM

Ambareen Siraj

Susan M. Bridges

Rayford B. Vaughn

Department of Computer Science

Mississippi State University

Msstate, MS 39762

e-mail: {ambareen, bridges, vaughn}@cs.mssstate.edu

Abstract

The "health" of a computer network needs to be assessed and protected in much the same manner as the health of a person. The task of an intrusion detection system is to protect a computer system by detecting and diagnosing attempted breaches of the integrity of the system. A robust intrusion detection system for a computer network will necessarily use multiple sensors, each providing different types information about some aspect of the monitored system. In addition, the sensor data will often be analyzed in several different ways. We describe a decision engine for an intelligent intrusion detection system that fuses information from different intrusion detection modules using a causal knowledge based inference technique. Fuzzy Cognitive Maps (FCMs) and fuzzy rule-bases are used for the causal knowledge acquisition and to support the causal knowledge reasoning process.

Keywords: intrusion detection, decision making, and fuzzy cognitive maps, causal knowledge inference.

1.0 Introduction

As computer technology advances and the threats of computer crime increase, the apprehension and preemption of such infractions become more and more difficult and challenging. Over the years, intrusion detection has become a major area of research in computer science. Intrusion detection systems are often characterized based on two aspects [1]:

- a) the data source (host based/ multihost based/ network based), or
- b) the model of intrusion detection (anomaly detection/ misuse detection).

There are wide variations in the techniques used by intrusion detection systems.

The Intelligent Intrusion Detection System (IIDS) is a prototype developed as part of an intrusion detection

research effort in the Department of Computer Science at Mississippi State University. The following unique features characterize IIDS:

- 1) Real time adaptive distributed and network based architecture.
- 2) Incorporation of both anomaly and misuse detection (i.e., misuse detection modules look for known patterns of attack while anomaly detection modules look for deviations from "normal" patterns of behavior [2]).
- 3) Integration of data mining algorithms with fuzzy logic and the use of genetic algorithms for optimization of membership functions and for feature selection [3,4].
- 4) Use of a decision engine to fuse information from different types of detection modules in order to make decisions about the overall health of the network.

The focus of this paper is the model of the decision engine that has been developed using causal knowledge inferencing via Fuzzy Cognitive Maps (FCMs). FCMs 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 [5]. Researchers have used FCMs for many tasks in several different domains. Among these are: disease diagnosis in the medical domain [6], fault management in distributed network environment [7], and failure modes effects analysis [8]. Smith and Eloff reported their work on enhanced risk assessment in a health care institution using cognitive fuzzy modeling: a combination of fuzzy cognitive models and fuzzy rule-based techniques [9].

In this paper we propose to use FCMs for decision support in the domain of network security and intrusion detection. FCMs are constructed to capture the causal knowledge that the decision engine uses for alert assessment in the network security environment. Section 2 describes the decision engine including the design goals and how it fits into the

This work was partially sponsored by the National Science Foundation Grant# CCR-9988524 and the Army Research Laboratory Grant # DAAD17-01-C-0011.

IIDS architecture. Section 3 describes the use of FCMs for decision support in an intrusion detection system. Section 3.1 provides a brief introduction to FCMs in general and section 3.2 discusses the FCM framework of the IIDS decision engine. Section 4 provides conclusions and describes future work.

2.0 Overview of the Decision Engine

The intelligent intrusion detection system (IIDS) architecture includes several unique fuzzy intrusion detection components [2]. In order to detect potential attack(s) and determine the overall network status, the decision engine fuses outputs from different intrusion detection modules serving as "experts". In the IIDS architecture, multiple components, both anomaly and misuse detection modules, monitor activities on individual workstations, activities of users, network traffic. These components pass information about suspicious behavior to the decision engine. The decision engine must then fuse and analyze the integrated information to determine the security status of individual workstations, the status of individual user accounts, and the status of the network as a whole.

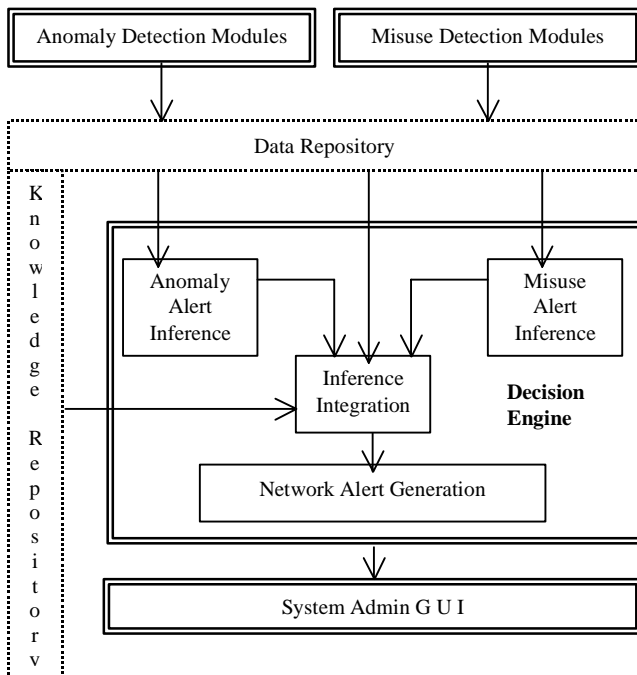


Figure 1: Decision Engine Framework

The responsibilities of the decision engine include the following tasks (Figure 1):

1. integration of network information from multiple detection components (both anomaly and misuse);

2. inference of individual machine and user status from various misuse detection components;
3. inference of network status from various anomaly detection components;
4. making decisions about the overall network status by combining information from all anomaly and misuse detection components;
5. alert decision trace-back to associated intrusion detection information; and
6. generation of network status reports for the security administrator.

3.0 Using Fuzzy Cognitive Maps for Decision Support

FCMs originated from the combination and synergism of fuzzy logic and neural networks, combining the robust properties of both [5]. A reasoning system using FCM is particularly attractive when compared to traditional rule-based reasoning systems because it simplifies the complicated and lengthy matching schemes and uses stronger mathematical analysis [7]. Professor Bart Kosko of the University of Southern California, proposed the idea of FCMs that are signed directed graphs for capturing causal knowledge and processing computational inference [10, 11, 12]. FCMs model the world as concepts and causal relations between concepts in a structured collection. Concepts (nodes) in an FCM are events that originate in the system and whose values change over time. Concepts take values in the interval $[0,1]$. The causality links between nodes are represented by directed edges that measure how much one concept impacts the other(s).

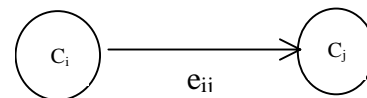


Figure 2. Two FCM concepts and a connecting edge representing a causal link

As shown in Figure 2, the edge value between concept C_i and C_j can be represented by e_{ij} . The weight associated with an edge takes values in the interval $[-1,1]$. An edge value of $e_{ij} = 0$ indicates that there is no relation between the concepts C_i and C_j . A value $e_{ij} > 0$ denotes positive causality—whenever concept C_i increases, C_j increases by the degree e_{ij} . Conversely, $e_{ij} < 0$ denotes negative causality—whenever concept C_i increases, there is a decrease in C_j by the degree e_{ij} . The higher the absolute value for e_{ij} , the greater the effect of the cause. FCMs can be successfully used to capture causal knowledge and to support causal inference [13].

3.2 FCMs in IIDS

We now describe a model of a decision engine incorporated in the intelligent intrusion detection system architecture that uses causal knowledge reasoning with FCMs. A primary task of the decision engine is to investigate the results generated by the misuse detection components that look at signatures of known attacks. For misuse detection, the IIDS uses rule-based detection mechanisms that work on each of the hosts of the network. Output from the misuse detection modules may be crisp or fuzzy. For certain types of attacks, the signature is either present or absent and the output of the module is binary. For other types of attacks like the number of failed logins, the output of the misuse detection module is a fuzzy measure of the degree of suspicion. The decision engine must assess results of the multiple misuse detection modules in order to compute the alert status for each machine and for each user account.

In this context, we use an FCM model that identifies several FCM concepts for each kind of misuse detection as different types of "suspicious events" that affect the machine and user alert level in different ways. Each of these suspicious events is triggered by the results of misuse detection modules. The events are activated with the help of a fuzzy rule-base where fuzzy rules are used to map multiple inputs to outputs. We can think of the concepts as fuzzy sets represented by fuzzy membership functions and the edges or links as fuzzy relations represented by one or more fuzzy rules.

The following simple example illustrates how an FCM can be used to capture a suspicious event pattern. Consider the following scenario: *the intruder is trying to access the network by breaking into a particular workstation. The intruder tries to login with several users' passwords and fails.* One can identify such an attack scenario by observing the number of login failures, the user and the machine

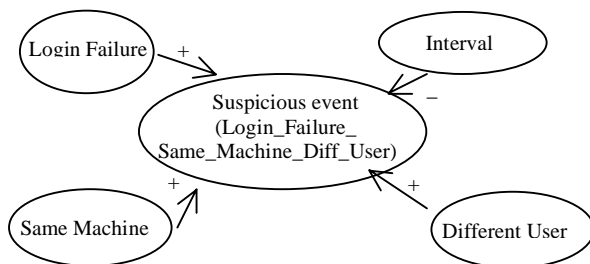


Figure 3. Example FCM for capturing misuse scenarios

involved, and the date and time of attack. This kind of attack should generate an alert for both - the machine and the user(s) concerned. Figure 3 shows an FCM that captures this scenario. The activation of the concept *Login_Failure_Same_Machine_Diff_User* by the other concepts can be implemented using a fuzzy rule-base. The fuzzy rules are used to map the multiple input concepts (the causes) to the output concept (the effect). Multiple fuzzy rules may be used to correspond to the knowledge described in an individual FCM. The FCM in Figure 3 can be implemented with a single fuzzy rule::

If *number of login failures* is moderate and *interval* is short and this happened for *same machine and different users* then, *Login_Failure_Same_Machine_Diff_User* is activated highly.

This kind of fuzzy cognitive modeling where fuzzy rules are used to support FCMs has been used for risk assessment in health care [9]. Carvalho and Tome report that rule-based FCMs are more effective than simple FCMs. Supporting fuzzy rules make FCMs fuzzy compatible and allows qualitative modeling [14].

For misuse inference, multiple FCMs capture different types of intrusive behavior as suspicious events. All suspicious events generated by the FCMs impact the machine and/ or user alert levels. However, the degrees of impact are different depending on the nature of the suspicious event. For example, a suspicious event due to *Login_Failure_Same_Machine_Same_User* should not impact the user alert level as much as a suspicious event due to *Login_Failure_Diff_Machine_Same_User*.

To fuse the impacts of the different suspicious events activated on behalf of different machines and users and to determine the alert status for the machines and the users, we exploit the resemblance of FCMs and neural networks. FCMs are in fact also known as "man trained" or "object oriented" neural networks [15]. In the neural network approach, the concepts are represented by neurodes and the edges are represented by the weights of the connecting neurodes. An adjacency matrix is used to list the cause and effect relationships between the nodes. The runtime operation is simply observed by determining the next value of each concept from the current concept and connecting edge values [15] and this can be represented as [12], for each concept C_i at t_{n+1} time,

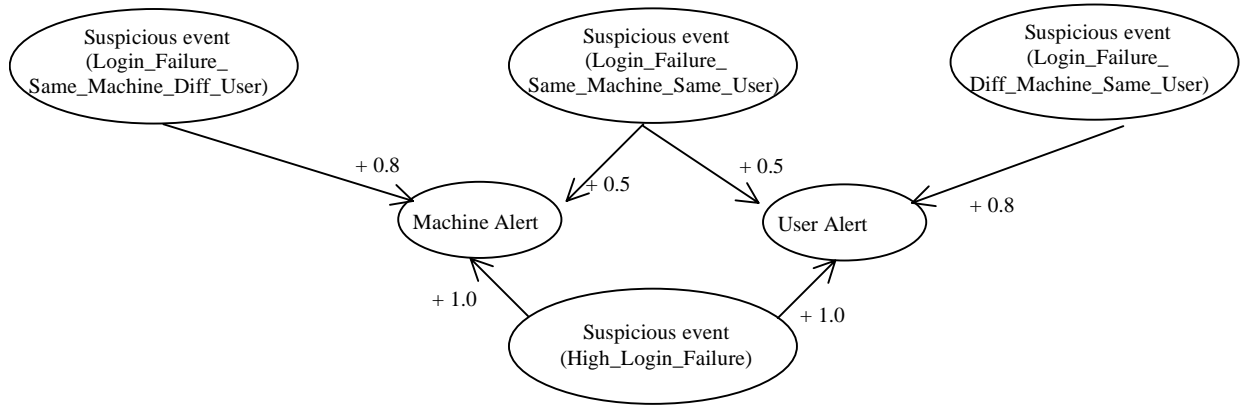


Figure 4. Combining evidence of multiple suspicious events

$$C_i(t_{n+1}) = S \left[\sum_{k=1}^n e_{ki}(t_n) C_k(t_n) \right].$$

A threshold function is used to force the concept value to be monotonically mapped into a normalized range. The threshold function that we use is the widely used sigmoid function [12] that transforms its input in the [0,1] interval and is of the form,

$$f(x) = \frac{1}{(1 + e^{-cx})}$$

Here, c is a constant such that $c > 0$ and determines the curve of the sigmoid function.

The suspicious events in the FCMs are treated as neurodes that trigger activation of the alert levels with different weights depicting causal relations between them. So, the alert value for particular machine or user reflects the degree to which it is operative in the system at a given time and is calculated as a function of all the activated suspicious events for that particular machine or user at that time. Figure 4 shows an example of a subset of FCMs that the decision engine employs in the IIDS architecture.

Generally, in FCMs, the edge values come from expert knowledge and experience. These are functions of the expert's common sense and engineering judgment [9]. Moreover, these parameters are tunable in FCM's flexible structure. A variety of both manual and automated techniques can potentially be used to fine-tune these parameters.

In the IIDS architecture, multiple anomaly detection sensors investigate network audit data. Current modules employ fuzzy data mining techniques with different approaches such as fuzzy association rules

and fuzzy frequency episodes [3]. The outputs of these modules are fuzzy measures of the "normality" of the audited data. One of the main tasks of the decision engine is to analyze the combined effect of the outputs of these anomaly detection modules in order to determine the network anomaly alert level.

For this purpose, FCMs are used to relate the causal relationship between the fuzzy measures that influence the anomaly alert level of the network.

The anomaly detection modules measure the dissimilarities between normal and abnormal data and report anomalous behavior in terms of an alarm percentage and a similarity measurement. In order to assess the combined effect of the outputs of the anomaly detection modules on the network's anomaly alert level, the decision engine uses causal analysis via FCMs. Figure 3 shows an example of such a FCM that can be used to infer the anomaly alert level of the network.

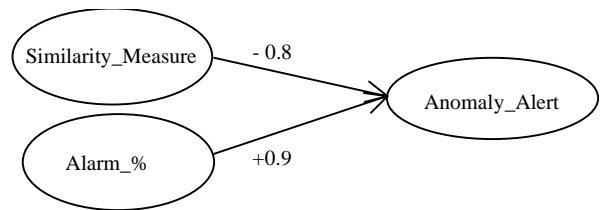


Figure 5. Example FCM for fusing anomaly detection results

Causal relations can be used to denote a set of fuzzy FCM rules [13]. The FCM in Figure 5 describes two such causal relations. One denotes that as the similarity measure increases, the anomaly alert level decreases with 0.8 causality. Intuitively this can mean that when the similarity measure is very high, the anomaly alert very low and, conversely, when the similarity measure is low, the anomaly alert is high.

Another FCM relation shows that alarm percentage increases the anomaly alert with 0.9 causality. So, if alarm percentage is high, then the anomaly alert is high, and likewise, if the alarm percentage is very low, than anomaly alert is very low. Thus, an FCM relation can replace many rules in a conventional rule-based system and FCM based reasoning is also semantically different than traditional reasoning [13].

For the task of combining information from multiple anomaly detection modules, the FCMs are represented and assessed by neural network approach. For misuse detection, linguistic FCMs are used to capture suspicious events that affect the machine and/or user alert level in various degrees and are analyzed with fuzzy rule-bases. The final task of the decision engine is to integrate the affects of the anomaly and misuse inferences to determine the overall network alert situation in order to detect possible intrusions indicated by combinations of seemingly harmless events. FCMs supported by fuzzy rules can also be used for this purpose. These FCMs deal with input or “cause” concepts such as machine and user alert levels, anomaly alert levels of network traffic and analyze the combined effect to determine the overall network alert status. This result is then reported to the security administrator.

FCMs help prevent certain kinds of knowledge extraction problems often encountered in traditional rule-based systems [16]. Modeling the decision process for the IIDS that fuses disparate outputs from various anomaly and misuse detection modules requires special attention. Using FCMs with greater flexibility makes sense in this context where dissimilar causes and effects are at play.

4.0 Summary and Conclusion

This paper described the design of a decision engine for an intelligent intrusion detection system that utilizes casual knowledge inference based on Fuzzy Cognitive Maps that are interesting and simple decision support tools. In the dynamic environment of the network security domain, using FCMs for decision support is attractive because FCMs are flexible and offer a practical yet natural knowledge acquisition scheme.

So far, we have used FCMs whose structure has been defined by human experts. Experiments are now ongoing that investigate the operational impact and effectiveness of employing this causal knowledge inferencing technique for decision support in the intelligent intrusion detection prototype. After we report on the effectiveness of using FCMs in our problem domain, we wish to explore how FCMs can

be learned and trained like neural networks in this context.

5.0 References

- [1] Carobs M. and K. Price. 1999. *Intrusion detection systems*. (<http://www.cerias.purdue.edu/coast/coast-library.html>)
- [2] Bridges. S. and R. Vaughn. 2000. Intrusion detection via fuzzy data mining. In *Proceedings of the 12th annual Canadian information technology security symposium held in Ottawa, June, 2000*, by Communications Security Establishment, 111 – 121
- [3] Luo, J. and S. M. Bridges 2000. , Mining fuzzy association rules and fuzzy frequency episodes for intrusion detection, *International Journal of Intelligent Systems*. 15(8): 687-703.
- [4] Shi, F. 2000. *Genetic algorithms for feature selection in an intrusion detection application* M.S. Thesis, Mississippi State University.
- [5] Stylios, C. and P. P. Groumpos. 2000. Fuzzy cognitive maps: a soft computing technique for intelligent control. In *Proceedings of the 2000 IEEE international symposium on intelligent control held in Patras, Greece, July, 2000*, 97 – 102.
- [6] Taber, R. 1991. Knowledge processing with fuzzy cognitive maps. *Expert Systems with Applications*. 1991(2): 83-87.
- [7] Ndousse, T. D. and T. Okuda. 1996. Computational Intelligence for distributed fault management in networks using fuzzy cognitive maps. In *Proceedings of the IEEE international conference on communications converging technologies for tomorrow's application, 1996*, 1558-1562. NY: IEEE.
- [8] Pelaez, C.E. and J.B. Bowles. 1995. Applying fuzzy cognitive maps knowledge representation to failure modes effects analysis. In *Proceedings of the IEEE annual symposium on reliability and maintainability, 1995*, 450-456.
- [9] Smith, E. and J. Eloff. 2000. Cognitive fuzzy modeling for enhanced risk assessment in health care institution. *IEEE Intelligent Systems and Their Applications*. March/ April 2000, 69-75.
- [10] Kosko, B. 1986. Fuzzy cognitive maps. *International Journal of Man-Machine Studies*. 1986 (24) : 65-75.
- [11] Kosko, B. 1992. *Neural networks and fuzzy systems: A dynamical systems approach to*

machine intelligence. Englewood Cliffs, NJ: Prentice Hall.

- [12] Kosko, B. 1997. *Fuzzy engineering*. Upper Saddle River , NJ: Prentice Hall.
- [13] Lee, K. C. and H. S. Kim. 1998. A causal knowledge driven inference engine for expert system. In *Proceedings of the annual Hawaii international conference on system science, 1998*. 284- 293.
- [14] Carvalho, J. P. and Jose A. B. Tome. 1999. Rule-based fuzzy cognitive maps and fuzzy cognitive maps- a comparative study. In *Proceedings of the 18th international conference of the North American fuzzy information, 1999*, by NAFIPS, 115 – 119.
- [15] Brubaker, D. 1996. Fuzzy cognitive maps. *EDN access*. 11 April, 1996.
- [16] Caudill, M. 1990. Using neural nets: fuzzy cognitive maps. *AI Expert*. 1990 (6): 49 -53.