Continuous Authentication by Keystroke Dynamics Using Committee Machines

Sergio Roberto de Lima e Silva Filho and Mauro Roisenberg

Informatics and Statistics Dept.
Federal University of Santa Catarina
P.O. Box 476 Campus Trindade 88040-900
Florianopolis, SC, Brazil
{sergio, mauro}@inf.ufsc.br
http://www.inf.ufsc.br/

1 Introduction

Current authentication mechanisms have a barely addressed problem: they only authenticate a user at the login procedure. If a user leaves the desk without logging out or locking computer session, an intruder has an occasion to use the system.

This paper proposes an authentication methodology that is both inexpensive and non-intrusive and authenticates users continuously while using a computer keyboard. The proposed methodology uses neural networks committee machines to recognize user's typing pattern, which is a biometric behavioral characteristic. The continuous authentication prevents potential attacks when user leaves the desk without logging out or locking computer session. Some experiments are done to evaluate and calibrate the authentication committee.

2 Methodology

The methodology proposed to authenticate users by keystroke dynamics can be divided into 2 steps: collecting data and modeling user template; and collecting data and classifying data to authenticate or to deny a user. In this study, we used as a structure representing users template a framework of ANNs grouped in a committee machine as can be seen in figure 1.

In order to represent each user template, a set of 13 ANNs sharing same topology are trained individually. The weights of this combination of ANNs become each user template. In the authentication step, data to be analyzed are presented to each network previously trained and a combination of all those ANNs outputs will decide whether the user is a valid one or is an intruder.

To provide training for the proposed committee machine, data from true user training set are presented as valid to each ANN. Accordingly, to each ANN invalid data set will be all other users training sets.

In order to define whether a given sample is valid or not, two variable thresholds were determined in the combination of committee machines. The first one

S. Mehrotra et al. (Eds.): ISI 2006, LNCS 3975, pp. 686–687, 2006.

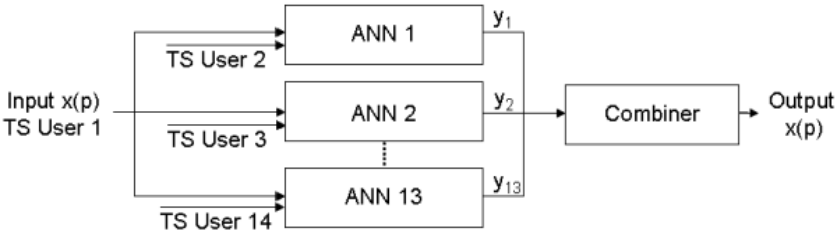

Fig. 1. Committee machine framework with the user 1 template

indicates which must be the minimum percentage of digraphs classified as valid ones by the committee machine. The second variable threshold is related to the number of ANNs that must classify data as valid.

3 Experiments and Results

In order to check proposed methodology performance some experiments were performed. These experiments used proposed committee machine to represent user template and user classification. In one of the experiments, thresholds are variable to each user committee machine classifier. The best results shown that a 0% FAR and a 0.15% FRR can be achieved, what was an excellent success rate when compared with other authentication methods. Other feature of the methodology is that new users can be easily added to the system, without the need to re-train all the Neural Networks.

4 Conclusions

From this study we can conclude that is possible to develop a secure, inexpensive, and continuous authentication method by behavioral characteristics of keystroke dynamics, using committee machines as classifiers.

Using ANNs in an adaptation of committee machines, the results obtained make possible to classify a user as true or intruder with accuracy comparable with other studies about the subject. From those results we can conclude that system effectiveness is improved using distinct thresholds for each user. Many studies in this research area show the need to re-training ANNs whenever a new user is added to the system as a major negative factor of using ANNs for authentication. This is the primary contribution of this study, because using committee machines there is no such need to re-train ANNs, we only have to train the ANNs that will constitute that user's committee machine and a new ANN for the committee machines of all the other users.