Oriental Journal of Computer Science & Technology Vol. **3**(2), 331-336 (2010)

Detecting terror- related activities on the web using neural network

DEEPAK TINGURIYA and BINOD KUMAR

Singanir University, District, Jhunjhunu - 333 515 (India).

(Received: October 12, 2010; Accepted: December 25, 2010)

ABSTRACT

Terrorist Detection System (TDS) is aimed at detecting suspicious users on the Internet by the content of information they access. TDS consists of two main modules: a training module activated in batch mode, and an on-line detection module. The training module is provided with web pages that include terror related content and learns the typical interests of terrorists by applying data mining algorithms to the training data. The detection module performs real-time monitoring on users" traffic and analyzes the content of the pages they access. An alarm is issued upon detection of a user whose content of accessed pages is "too" similar to typical terrorist content. TDS feasibility was tested in a network environment. Its detection rate was better than the rate of a state of the art Intrusion Detection System based on anomaly detection. In this Paper we present an Neural based Self organization map algorithm in TDS, where the detection algorithm was enhanced to improve the detection and reduce the false alarms in Terrorist Detection System

Key words: Terrorist detection system, neural network, data mining.

INTRODUCTION

The Internet is an efficient communication infrastructure that is increasingly used by terrorist organization to safely communicate with their affiliates, coordinate action plans, spread propaganda message, raise funds, and introduce supporters into their networks. Government and intelligence agencies are calling to invest major efforts in development of new method and technologies for identifying terrorist activities on the web in order to prevent future acts of terror. TDS Present and example to such an effort

By means of content monitoring and analysis of web pages accessed by a group of web user, it is possible to infer their typical areas of interest. It is also possible to identify users that access specific, potentially illegitimate information on the internet. Using this approach, real time web traffic monitoring may be performed to identify terrorist as they access typical terror related content on the internet.

Many terror-related groups use the Web as a convenient, anonymous communication infrastructure. This infrastructure enables exchange of information and propagation of ideas to active and potential terrorists. The Terrorist Detection System (TDS) is aimed at tracking down suspected terrorists by analyzing the content of information they access.

Terrorist cells are using the Internet infrastructure to exchange information and recruit new members and supporters. For example, high-speed Internet connections were used intensively by members of the infamous 'Hamburg Cell' that was largely responsible for the preparation of the September 11 attacks against the United States. This is one reason for the major effort made by law enforcement agencies around the world in gathering information from the Web about terror-related activities. It is believed that the detection of terrorists on the Web might prevent further terrorist attacks One way to detect terrorist activity on the Web is to eavesdrop on all traffic of Web sites associated with

terrorist organizations in order to detect the accessing users based on their IP address. Unfortunately it is difficult to monitor terrorist sites (such as 'Azzam Publications' since they do not use fixed IP addresses and URLs. The geographical locations of Web servers hosting those sites also change frequently in order to prevent successful eavesdropping. To overcome this problem, law enforcement agencies are trying to detect terrorists by monitoring all ISPs traffic (Ingram 2001), though privacy issues raised still prevent relevant laws from being enforced.

Terrorist Detection System (TDS)

TDS is a content based detection system recently developed to detect users who are interested in terror related pages on the web by monitoring their online activities. The system is based on real time monitoring of internet traffic of defined group of web users. The group is suspected to include hidden individual terrorists and the system aims at detecting them. The current version of TDS refers only to the textual content of the accessed web pages. It consists of two main modules: *a training module* activated in batch and a real time *detection module*

The training module receive as input a set of web pages that include terror related content. It applies cluster analysis on the textual representation of each page resulting with an asset of vector that efficiently represents typical terrorist's area of internet.

The detection module performs on line monitoring of all traffic between the users being monitored and the web. The content of the pages they access is analyzed, transformed to a form of a vector. And added to the vector representing the user profile. The profile for each user is kept during a period of time and number of transactions defined by operative system parameters. Similarity is measured between each users profile and the typical terrorist areas of interest. A consistent high similarity between specific users and terror related content would raise an alert about those users. Each user related to the monitored group is identified by a user's computer having a unique IP Address. In case of real time alarm, the detected IP can be used to locate the suspicious computer and hopeful the suspected user who may still be logged on to the same computer .

The detection module, being activated in real time, it required to efficiently capture the textual content t of web page form the internet traffic, actually , the detection efficiency is crucial to TDS effectiveness skipped pages or inaccurate analysis of pages due to slow handling of traffic might result in unreliable detection .

In this Paper we present a Neural based algorithm in TDS, where the detection algorithm was enhanced to improve the detection and reduce the false alarms in Terrorist Detection System.

Background

This research integrates issues from the research fields of computer security (Intrusion Detection Systems), information retrieval (the vector-space model), and data mining (cluster analysis). The following subsections include a brief overview of these topics and their relation to the newly proposed methodology.

Intrusion Detection System

An Intrusion Detection System (IDS) constantly monitors actions in a certain environment and decides whether they are part of a possible hostile attack or a legitimate use of the environment.The environment may be a computer, several computers connected in a network or the network itself. The IDS analyzes various kinds of information about actions emanating from the environment and evaluates the probability that they are symptoms of intrusions. Such information includes, for example, configuration information about the current state of the system, audit information describing the events that occur in the system (e.g., event log in Windows XP), or network traffic. Several measures for evaluating IDS have been suggested (Debar *et al.* 1999; Richards 1999; Spafford and Zamboni 2000; Balasubramaniyan *et al.* 1998). These measures

Include accuracy, completeness, performance, efficiency, fault tolerance, timeliness, and adaptively. The more widely used measures are

The True Positive (TP) rate, that is, the percentage of intrusive actions (e.g., error related pages) detected by the system, False Positive (FP) rate which is the percentage of normal actions (e.g., pages viewed by normal users) the system incorrectly identifies as intrusive, and Accuracy which is the percentage of alarms found to represent abnormal behavior out of the total number of alarms. In the current research TP, FP and Accuracy measures were adopted to evaluate the performance of the new methodology.

Vector-Space Model

One major issue in this research is the representation of textual content of Web pages. More specifically, there is a need to represent the content of terror-related pages as against the content of a currently accessed page in order to efficiently compute the similarity between them. This study will use the vector-space model commonly used in Information Retrieval applications for Representing terrorists' interests and each accessed Web page. In the vector-space model, a document d is represented by an n dimensional vector d = (w1,w2,…..,wn), where wi represents the frequency-based weight of term i in document d. The similarity between two documents represented as vectors may be computed by using one of the known vector distance measuring methods such as Euclidian distance or Cosine (Boger, *et al.* 2001; Pierrea, *et al.* 2000). In this study each Web page in considered as a document and is represented as a vector. The terrorists' interests are represented by several vectors where each vector relates to a different topic of interest. The cosine similarity measure is commonly used to estimate the similarity between an accessed Web page and a given set of terrorists' topics of interests.

Clustering Techniques

Cluster analysis is the process of partitioning data objects (records, documents, etc.) into meaningful groups or clusters so that objects within a cluster have similar characteristics but are dissimilar to objects in other clusters. Clustering can be viewed as unsupervised classification of unlabelled patterns (observations, data items or feature vectors), since no pre-defined category labels are associated with the objects in the training set. Clustering results in a compact representation of large data sets (e.g., collections of visited Web pages) by a small number of cluster centroids. Applications of clustering include data mining, document retrieval, image segmentation, and pattern classification (Jain *et al.* 1999). Thus, clustering of Web documents viewed by Internet users can reveal collections of documents belonging to the same topic. As shown by Sequeira and Zaki (2002), clustering can also be used for anomaly detection: normality of a new object can be evaluated by its distance from the most similar cluster under the assumption that all clusters are based on 'normal' data only.

A good clustering method will produce high quality clusters in which similarity is high known as intra-classes and inter-classes where similarity is low. The quality of clustering depends upon both the similarly measure used by the method and it, s implementation and it is also measured by the it, s ability to discover hidden patterns.

The concept of clustering algorithms is to build a finite number of clusters, each one with its own center, according to a given data set, where each cluster represents a group of similar objects. Each cluster encapsulates a set of data and here the similarities of the surrounded data are their distance to the cluster center.

Generally speaking, clustering techniques can be divided into two categories pair wise clustering and central clustering. The former also called similarity-based clustering, groups similar data instances together based on a data-pair wise proximity measure. Examples of this category include graph partitioning-type methods. The latter, also called centroid-based or model-based clustering, represents each cluster by a model, i.e., its centroid".

Central clustering algorithms are often more efficient than similarity-based clustering algorithms. We choose centroid-based clustering over similarity-based clustering. We could not efficiently get a desired number of clusters, e.g., 100 as set by users. Similarity-based algorithms usually have a complexity of at least $O(N2)$ (for computing the data-pair wise proximity measures), where N is the number of data.

Content – Based Detection of Terror Related Activity

Detection Environment

This study suggests a new type of knowledge-based detection methodology that uses the content of Web pages browsed by terrorists and their supporters as an input to a detection process. In this study, refers only to the textual content of Web pages, excluding images, music, video clips, and other complex data types. It is assumed that terror-related content usually viewed by terrorists and their supporters can be used as training data for a learning process to obtain a 'Typical-Terrorist-Behavior'. This typical behavior will be used to detect further terrorists and their supporters. A 'Terrorist-Typical-Behavior' is defined as an access to information relevant to terrorists and their supporters. A general description of a system based on the suggested methodology is presented in Figure 1. Each user under surveillance is identified as a 'user's computer' having a unique IP address rather than by his or her name. In the case of a real-time alarm, the detected IP can be used to locate the computer and hopefully the suspected terrorist who may still be logged on to the same computer.

The suggested methodology has two modes of operation:

Learning typical terrorist behavior

In this mode, a collection of Web pages from terror related sites is downloaded and represented as a set of vectors using the vector space model. The collected data is used to derive and represent the typical behavior of the terrorists and their supporters by applying techniques of unsupervised clustering. Since the IP addresses of downloaded pages are ignored, moving the same or similar contents to a new address, as frequently carried out by error related sites, will not affect the detection accuracy of the new method.

Monitoring users

This mode is aimed at detecting terrorist users by comparing the content of information accessed by users to the Typical-Terrorist–Behavior. The textual content of the information accessed by a user on the Web is converted into a vector called 'access vector'. An alarm is issued when the similarity between the 'access vector' and the Typical- Terrorist-Behavior is above a predefined threshold. The privacy of regular users is preserved, since the system does not need to store either the visited IP addresses or the actual content of the viewed pages. Due to extensive dimensionality reduction procedures, the access

Vectors do not hold sufficient information to restore the actual content of the page. Other types of viewed content (e.g., images) are ignored by the system. Apparently the task of making a distinction between a legitimate user and a terrorist is a typical classification problem with two alternative classes: terrorists vs. no terrorists.

However, the most popular classification algorithms are probabilistic in their nature, i.e., they assume a stable and relatively balanced probability distribution of classes over the entire

Population. Moreover, they usually ignore any differences between the misclassification costs of objects belonging to different classes. All these assumptions are totally wrong when dealing with terrorist detection on the Web. The monitored population is completely unbalanced so that the actual percentage of terrorists in the entire population of Web users is usually close to zero. Consequently, in this study it was decided to follow the more flexible clustering approach to terrorist detection, while leaving the Investigation of classification methods to future Research

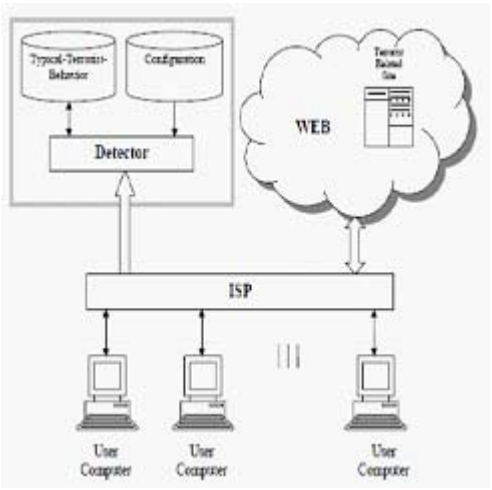

Fig. 1: Detection Environment

Proposed Approach

Self-Organizing Map (SOM)

The Self-Organizing Map [7] is a neural network model for analyzing and visualizing high dimensional data. It belongs to the category of competitive learning network. The SOM defines a mapping from high dimensional input data space onto a regular two-dimensional array of in designed architecture is input vector with six input values and output is realized to 2 dimension spaces. Every neuron i of the map is associated with an n-dimensional reference vector [m_1,m_2..m_n] where n denotes the dimension of the input vectors. The reference vectors together form a codebook. The neurons of the map are connected to adjacent neurons by a neighborhood relation, which dictates the topology, or the structure, of the map.

Adjacent neurons belong to the neighborhood Ni of the neuron i. In the SOM algorithm, the topology and the number of neurons remain fixed from the beginning.

The number of neurons determines the granularity of the mapping, which has an effect on the accuracy and generalization of the SOM. During the training phase, the SOM forms elastic net that is formed by input data. The algorithm controls the net so that it strives to approximate the density of the data. The reference vectors in the codebook drift to the areas where the density of the input data is high.

The Learning Algorithm of the SOM

There are some basic steps involved in the application of the SOM algorithm. Firstly the weights of the network should be initialized. Assigning them small values picked from a random number generator can do this; in doing so, no prior order is imposed on the feature of map. The only restriction is that the weight vector, wj(0) should be different for j = 1, 2, . . . , n, where n is the number of neurons in the lattice.

An alternative way of initializing the weight vector is to select from the available set of input vectors in a random manner. The key point is to keep the magnitude of the weights small, because the initial weights already give good approximation of the SOM weights. Next step is the similarity matching. With the use of the Euclidean minimum-distance criterion, the distance from the training data set to all weight vectors are computed and based on these computations the BMU is found.

The Euclidean formula is given by

$$I(x)=\text{argmin}\|x(n)-w_j\|,\ j=1,2\ldots n$$

Where I(x) identifies the best matching neuron to the input vector x. In words this formula finds the weight vector most similar to the input vector, x. This process sums up the essence of the competition among the neurons. In the sense of network topology there is a mapping process involved with this competition;

A continuous input space of activation patterns is mapped onto a discrete output space of neurons by a process of competition among the neurons of the network [6].

After having found the winning neuron the next step of the learning process is the updating. The weight vector of the winning neuron and the neurons close to it in the SOM lattice are adjusted towards the input vector. The update formula for the neuron j at time (i.e., number of iteration) n with weight vector w_j (n) is

$$w_j(n+1)=w_j(n)+h(n)h_{j,i(x)}(n)(x-w_j(n))$$

Where h(n) is the learning-rate parameter and hj, i(x) (n) is the time-varying neighborhood function centered around the winning neuron I(x). A typical choice of hj,i(x) is the Gaussian function [7] [8], which is given by the formula

$$h_{i,i(\mathbf{x})}(n) = \exp\left(-\frac{d_{j,i}^2}{2\sigma^2(n)}\right)$$

where h(n) is a width function and dj,i represents the distance between the winning neuron i and its neighbor neuron j. The whole process is repeated for each input vector over and over for a number of cycles until no noticeable changes in the feature map are observed or a certain number of approaches are reached. Where h(n) is the learning-rate parameter [8] and hj, i(x) (n) is the time-varying

neighborhood function centered around the winning neuron i(x).

Evaluation Measures

To evaluate the system performance the following measures (based on Sequeira and Zaki 2002) were used.

True Positive Rate (TP) (also known as Detection Rate or Completeness): the percentage of terrorist pages receiving a rating above the threshold in the experiments, terrorist pages will be obtained from the users simulating terrorists.

False Positive Rate (FP): the percentage of regular Internet access pages that the system incorrectly determined as related to terrorist activities, i.e., the percentage of non-terrorist pages receiving a rating above threshold and suspected falsely as terrorists. *Accuracy* – percentage of alarms related to terrorist behavior out of the total number of alarms. Since no benchmark data on content based intrusion detection is currently available, the results are compared to the best numbers achieved with ADMIT which is a command level method using the Means clustering algorithm to detect intruders (Sequeira and Zaki 2002).

CONCLUSION

In this work, we study the possible use of the neural networks learning capabilities in Terrorist Detection System. an innovative, knowledgebase

Methodology for terrorist activity detection on the Web is presented. Neural Network methodology can be useful for detecting terrorists and their supporters using a legitimate ways of Internet access to view terror related content at a series of evasive web sites. The detection methodology presented here can be applied to detecting other types of criminals surfing the Web such as pedophiles accessing child pornography sites.

REFRENCES

1. Mahesh s,Mahesh T R, M Vinayababu, " Using Data Mining Techniques for Detecting terror related activities on the web", *Journal of Theoretical and Applied information technology* (2010).
2. Abbasi, A. and Chen, H., Applying authorship analysis to extremist group Web forum messages. IEEE Intelligent Systems, Special Issue on *Artiûcial Intelligence for National and Homeland Security*, **20**(5): 67–75 (2005).
3. Baumes, J., Goldberg, M., Hayvanovych, M., Magdon-Ismail, M., Wallace, W., & Zaki, M., Finding hidden group structure in a stream of communications. In S. Mehrotra, D.D. Zeng, & H. Chen (Eds.), Proceedings of the IEEE Conference on Intelligence and Security Informatics (pp. 201–212). Los Alamitos, CA: IEEE (2006).
4. Chen, H., Intelligence and security informatics: Information systems perspective. Decision Support Systems: Special Issue on Intelligence and Security Informatics, **41**(3): 555–559 (2006).
5. Chen, H., Qin, J., Reid, E., Chung, W., Zhou, Y., Xi, W., et al., The dark Web portal: Collecting and analyzing the presence of domestic and international terrorist groups on the Web. In W.T. Scherer & B.L. Smith (Eds.), Proceedings of the 7th IEEE International Conference on Intelligent Transportation Systems, (pp. 106–111). Los Alamitos (2004).
6. Report to Congress Regarding the Terrorism Information Awareness (TIA) Program. Submitted by the Secretary of Defense, Director of Central Intelligence and Attorney General, (2003).