Design of an Artificial Immune System as a Novel Anomaly Detector for Combating Financial Fraud in the Retail Sector

Jungwon Kim, Arlene Ong and Richard E Overill
Department of Computer Science,
King's College London,
Strand, London WC2R 2LS, U.K.
{jungwon, ong, reo}@dcs.kcl.ac.uk

Abstract- The retail sector often does not possess sufficient knowledge about potential or actual frauds. This requires the retail sector to employ an anomaly detection approach to fraud detection. To detect anomalies in retail transactions, the fraud detection system introduced in this work implements various salient features of the human immune system. This novel artificial immune system, called CIFD (Computer Immune system for Fraud Detection), adopts both negative selection and positive selection to generate artificial immune cells. CIFD also employs an analogy of the self-Major Histocompatability Complex (MHC) molecules when antigen data is presented to the system. These novel mechanisms are expected to improve the scalability of CIFD, which is designed to process gigabytes or more of transaction data per day. In addition, CIFD incorporates other prominent features of the HIS such as clonal selection and memory cells, which allow CIFD to behave adaptively as transaction patterns change.

Keywords: self-MHC, positive selection, negative Selection, anomaly detection, fraud detection

1 Introduction

As many business sectors in the UK and Europe move towards implementing e-commerce solutions, and come to rely ever more heavily upon open systems and networks, the potential for fraud and related criminal activities is greatly increased. In order to promote the move towards secure e-commerce, research aimed at providing efficient and effective fraud detection is being pursued with increasing vigour (AAAI, 2002).

The financial fraud problem studied in this paper is set in the retail business sector, where business transactions are handled electronically. As a result, they are potential targets for various fraudulent activities. However, the retail sector often does not possess sufficient expertise about potential or actual frauds. This requires the retail sector to employ an anomaly detection approach to fraud detection.

In order to develop a fraud detection system (FDS) to meet the new requirement for detecting retail business fraud, this paper introduces a novel fraud detection approach implementing analogies of various salient features of the human immune system (HIS). The negative selection algorithm is the most well known artificial immune system (AIS) that has been popularly used for anomaly detection (De Castro and Timmis, 2002). However, a recent study shows a scaling problem with this algorithm when it is used to monitor a large amount of real data (Kim and Bentley, 2001). This problem motivates this study to propose a new AIS, which can detect anomalies from a huge volume of retail transaction data.

The novel AIS, called CIFD (Computer Immune system for Fraud Detection), implements negative selection and positive selection together to generate artificial immune cells. In addition, it employs the analogy of the self-Major Histocompatability Complex (MHC) molecules in order to present antigen data to the system. These novel features are introduced in order to improve the scalability of CIFD. In addition, CIFD accommodates other salient features of the HIS, which are often implemented by AIS such as clonal selection and artificial memory cells. These features allow CIFD to behave adaptively as transaction patterns change.

In the next section, we present a brief review of financial fraud in the retail sector. Section 3 introduces the T-cell development process of the HIS and section 4 describes how CIFD implements the T-cell development process introduced in section 3. Then, section 5 gives an overview of the conceptual architecture of the CIFD system, and section 6 discusses related work with the HIS analogy CIFD has used with respect to the system scalability. Finally, section 7 presents further work with our interim conclusions.

2 Financial Fraud in Retail Business

In order to develop an effective fraud detection system (FDS), the appropriate monitoring targets of the FDS should first be identified. The potential frauds within a large retail business can be broadly classified into two categories: fraud against the business itself, and fraud against its clients via its systems. The CIFD system presented in this paper focuses on detection of frauds in the former category. This type of fraud, which is against

the business itself, can also be categorised into three groups according to the potential parties committing the fraud. They are customers (users of the services), employees who are regular users of the retail transaction processing system (RTPS), and other employees who are not normally users of the RTPS but have legal access to it. The second group was selected as the most suitable monitoring target for CIFD for the following reasons:

- Customers using the services would be more easily able to commit fraud against the selected business's clients than against the business itself.

- Other employees with legal access to RTPS who wish to commit fraudulent activities would probably have to do so in conspiracy with the employees who use the system in order to obtain cash or stock.

Thus, it is believed that the focus of CIFD on monitoring internal users of the RTPS greatly reduces the overall complexity of the task without seriously compromising the effectiveness of the system. A typical example of a fraud that is committed by the internal users of the RTPS is the entry of fake transactions. The internal users, who are employees of an outlet, are paid proportionally according to the number of transactions they process per day. Hence, it is often found that they spread a possible transaction into several transactions, causing the retail business owner to overpay. However, other than this simple example, the end-users of CIFD do not posses much detailed knowledge of frauds.

Because of these reasons, CIFD aims to detect anomalies in product sales patterns, made from the transactions entered by the internal users of RTPS. The basic concept of detecting anomalous product sales patterns is to look for patterns that appear to be significantly different from normal product sales patterns observed from data collected previously.

3 Supplementing Negative Selection for T-cell Maturation

3.1 Negative Selection Algorithm

CIFD aims to detect non-self product sales patterns by discerning those patterns that are not regarded as normal. T-cells in the HIS are a type of immune cell which plays a leading role in dicriminating between self and non-self cells. Alongside the ability to detect non-self antigens, T-cells also have a key feature called *self-tolerance*: not reacting to self antigens. One explanation of how T-cells achieve self-tolerance is given by negative selection (Tizard, 1995). At the thymus, immature T-cells develop into mature T-cells and negative selection occurs during this process. During negative selection, immature T-cells in the thymus are tested to see if they bind to self antigens. If the T-cells bind to any self antigens they are eliminated, otherwise they become mature. Mature T-cells are then distributed to lymph nodes and start detecting non-self antigens. Mature T-cells which pass a negative selection test are believed to bind to only non-self cells without binding to self-cells.

Negative selection of T-cells inspired the development of the negative selection algorithm (Forrest et al., 1997). The algorithm has been popular in various applications for anomaly detection purposes (De Castro and Timmis, 2002). However, this appealing approach shows scaling problems when it is applied to a large amount of real data (Kim and Bentley, 2001). Since the publication of Kim and Bentley's work, many other studies have reported similar problems and proposed potential solutions (Ayara, , *et al.*, 2002; Lamont, *et al.*, 1999; Dasgupta and Gonzalez 2002; Esponda, Forrest, and Helman, 2003). Although these new suggestions provide possible options for tackling the scaling problem of the negative selection algorithm, none of them has yet reported that a new approach that actually scales to a huge amount of data, whose size in real applications may reach several gigabytes or more.

3.2 T-cell Maturation

In order to solve the above problem, we pay attention to the other T-cell selection process occurring during T-cell maturation. The maturing process of T-cells in the thymus consists of two selection stages: positive and negative selections (Sompayrac, 1999). Whilst negative selection is crucial, to provide self-tolerance to the HIS, positive selection is needed for T-cells to recognise the self-Major Histocompatability Complex (MHC). The antigens presented to T-cells for binding are carried by Antigen Presenting Cells (APCs). APCs are special cells that engulf antigens distributed throughout a body and convey them to T-cells for binding. In addition, APCs transform engulfed antigens to a specific form that allows T-cells to bind to them. The MHC molecules of APCs perform a key role in this transformation. MHCs sample the fragments of

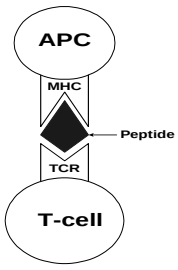

Figure 1. MHC/peptide bind to TCR

antigen proteins (called peptides) inside APCs and carry them to the surfaces of APCs. Then, actual binding between antigens and T-cells occurs between T-cell receptors (called TCR) and MHC/peptide bindings on APC surfaces (figure 1). MHCs are known to be unique to each individual and therefore provide a marker of 'self'. Hence, the MHC of each individual is called the self-MHC.

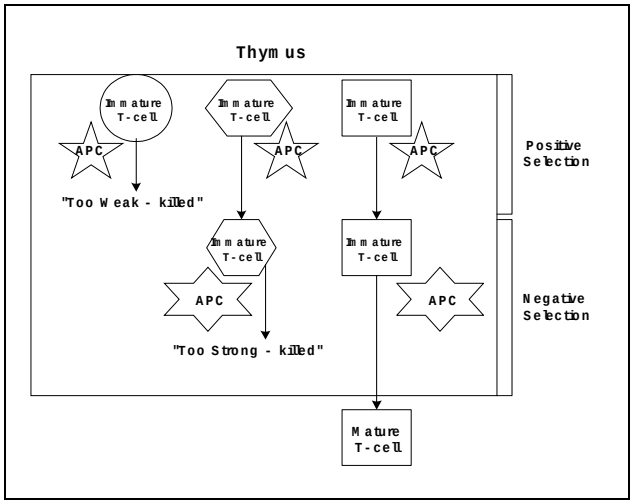

Figure 2. Positive selection and negative selection

Returning to the maturation of T-cells, unlike negative selection, positive selection selects only T-cells that bind to self-MHC/peptide bindings on APCs in the thymus. In other words, T-cells which do not bind to self-MHC/peptide bindings on APCs are eliminated. Figure 2 shows this process together with negative selection[1]. The immunology literature explains the role of positive selection as providing T-cells with self-MHC restriction (Tizard, 1995; Sompayrac, 1999). The self-MHC restriction ensures that all mature T-cells can recognise antigen peptides in the context of self-MHC. This feature concerns the activation focus of T-cells. For instance, the uninfected self-cells having virus-debris stuck on their surfaces could activate T-cells if T-cells did not have the self-MHC restriction feature. However, with the self-MHC restriction feature, T-cells only activate when they can bind to peptides carried by self-MHC from the inside of infected cells. That is to say, positive selection eliminates useless T-cells that cannot activate later.

Whilst positive selection provides a useful feature together with negative selection, there is a question to be answered. How can a T-cell, which binds to self-MHC/peptides during positive selection, pass negative selection, which requires it not to bind to self-MHC/peptides? There are several models attempting to explain this point, but none of them yet provides a clear answer (Sompayrac, 1999). However, the common thinking among these models is that the strength of binding between self-MHC/peptide and TCR (known as the *affinity* of a T-cell) determines a pass or a failure of the two selection tests. For instance, T-cells binding self-MHC/peptides with relatively weak affinities are selected from positive selection. Among T-cells selected from positive selection, those whose affinities are relatively strong are discarded during negative selection. Therefore, T-cells whose affinities are not too strong to be activated by self-antigens, but not too weak to be ignored by self-MHC become mature T-cells.

Through the self-MHC restriction and self-tolerance, T-cells are able to recognise foreign invaders without attacking self-antigens. We believe that a T-cell maturation process including the positive and negative selection together with self-MHC may possibly help to reduce the lengthy computing time of AIS based solely on the negative selection algorithm. A novel AIS, CIFD, proposed here adopts a T-cell maturation process consisting of positive selection and negative selection alongside self-MHC. We hope that the self-MHC restriction feature of artificial T-cells, which is provided by self-MHC and positive selection, contributes to improve the scalability of CIFD. In addition, CIFD accommodates other salient features of the HIS, which are often implemented by AIS, such as clonal selection and artificial memory cells. The overall conceptual architecture of CIFD is introduced in section 5.

4 CIFD Implementation of T-detector Maturation

This section introduces how self-MHC, positive selection and negative selection described above are implemented within CIFD. Contrary to many other approaches (De Castro and Timmis, 2002), we do not attempt to develop CIFD using the exact mechanisms of the HIS. Rather, we only mimic them at a high level of abstraction and employ other available data mining algorithms for actual implementation.

4.1 Self-MHC

Self-MHC pre-processes a given antigen to be in an appropriate form to bind TCR of mature T-cells. Association rule mining is CIFD's equivalent of self-MHC. Association rule mining automatically discovers interesting associations or correlations among a large number of possible attribute values. It selects frequent itemsets [2] whose frequency of occurrence (known as *support*) is above a minimum threshold. These frequent itemsets are then represented in an "If-Then" rule form by inserting "If" and "Then" between items. Among these rules, those whose accuracy (known as *confidence*) is above a minimum threshold are finally selected. For instance, the most commonly used association rule-mining algorithm, *Apriori* (Agrawal and Srikant, 1994), generates rules such as "*If* milk *Then* bread with confidence = 70%" from supermarket sales transaction data. This rule implies

[1] The order of occurrence of these two selection stages is not known yet (Sompayrac, 1999). As a simplifying illustration of these stages, we arbitrarily put positive selection before negative selection.

[2] An item is a specific pair of {attribute *i*, existing value *j* of attribute *i*) and an itemset is a collection of such items. For instance, "Quantity = 100" is an item and {Quantity = 100, Employee-ID = 200} is an itemset.

HIS	Role	CIFD	Role
Self-MHC Molecule	Sample the fragments of antigens and carry them on the surface of APCs	Association Rule Mining Algorithm	Extract frequent transaction patterns from input antigen data and provide them to CIFD as input
Self-MHC/Peptide bindings	Antigen binding areas of T-cells	Strong association rules	Antigen data patterns that bind T-detectors
Positive Selection	Provide self-MHC restriction by generating immature T-cells that bind self-MHC/peptides with relatively weak affinities	Generate Immature T-Detectors	Provide self-MHC restriction by generating immature T-detectors that binds the IF part of strong association rules.
Negative Selection	Provide self-tolerance by eliminating immature T-cells that bind self-MHC/peptides with strong affinities	Generate Mature T-Detectors	Provide self-tolerance by generating mature T-detectors whose distance to conflicting strong association rules is large.
Self-MHC Diversity	High diversity provides a greater chance for non-self antigen peptides to bind self-MHC	Calendar Schema	Increase the granularities of association rules so that it provides a greater chance for non-self antigen data to bind T-detectors

Table 1 Comparison between the human immune system(HIS) and CIFD.

that a shopper buying milk is 70% likely to purchase bread as well.

The motivation for using association rule mining as self-MHC is twofold: scalability and feature construction. *Apriori* offers a clever strategy to increase scalability. It uses the *monotonic* property of frequent itemsets: an itemset can be frequent only when all of its subset itemsets are frequent. This property allows *Apriori* to filter out itemsets as soon as they have an infrequent subset itemset (Agrawal and Srikant, 1994). As a result, the total number of itemsets whose supports need to be counted is greatly reduced. This feature makes *Apriori* an efficient algorithm and it has become very popular. In addition, Lee (1999) showed that *Apriori*-based association rule mining algorithms are competent at constructing meaningful new features when the original data format does not necessarily provide expressive features reflecting normal patterns. These features are analogous to those offered by the self-MHC of the HIS. As the self-MHC carries the hidden antigen peptides onto the APC surface in a visible form, *Apriori* constructs meaningful features of antigen data in an intelligent form as an "If-Then" rule.

In addition, *Apriori* selects *strong* association rules, whose confidences are above a pre-defined threshold, as a final rule set. Strong association rules generated by *Apriori* reflect "frequent transaction patterns". These are the self-MHC/peptide bindings of CIFD, which would be presented to bind T-detectors. This means that self-MHC/peptide bindings of CIFD, which are strong association rules, represent "frequent transaction patterns".

4.2 Positive Selection and Negative Selection

In order to perform positive and negative selection, CIFD must first generate immature artificial T-cells, called *T-detectors*. The best-known approach to generating immature T-detectors for AIS is pseudo-random generation (De Castro and Timmis, 2002). Some later works by (Ayara *et al.*, 2002; Lamont *et al.*, 1999; Dasgupta and Gozalez, 2002) also suggest different approaches in order to generate immature T-detectors in a more efficient way. However, none of these works seem to be efficient enough to scale up to the volume of data provided to CIFD. CIFD is designed to monitor sales transactions involving 19,700 UK outlets and 2,723 distinct products; each transaction record contains 23 fields, giving a total of 1.6GB data/day. The immediate challenge to be tackled by this work is therefore developing a system that can scale up to this huge volume of data. This requires CIFD to have both positive and negative selection implementation in a modified way.

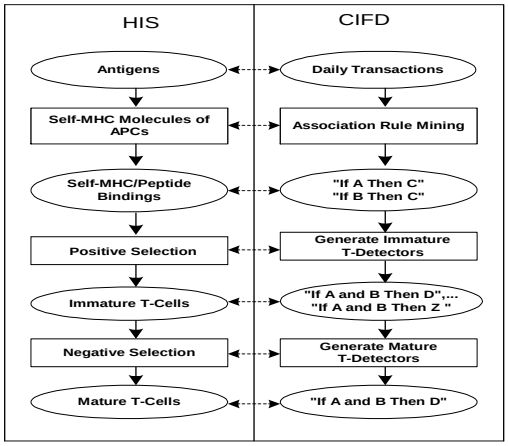

Figure 3. Generate T-detectors

Instead of randomly generating an immature T-detector, CIFD generates an immature T-detector in the form of an "If-Then rule" that contradicts given self-MHC/peptides. More specifically, it generates an immature T-detector by combining two strong association rules which share the same consequent (the "Then" part of a rule) (Hussain *et al.*, 2000). For instance, let two strong rules presented as self-MHC/peptides to the "Generate Immature T-detectors" process in figure 3 be "If A Then C" and "If B Then C". An immature detector is generated by having an antecedent (the "If" part of a rule) that combines the two antecedents of the rules and a

consequent that contradicts the consequent of the two rules. Hence, an immature detector generated from the above two strong rules would be "If AB Then not C". Since there can be more than one value representing "not C" as the consequent of this rule, a set of immature detectors would be {"If AB Then D", "If AB Then E",....}. However, among these rules, some rules do not follow a CIFD self-context, analogous to immature T-cells discarded by positive selection, and they can be filtered by applying a rule confidence threshold. Only the immature T-detectors whose confidences are higher than a pre-defined threshold are selected. The "Generate Immature T-detectors" process in figure 3 indicates this process. This process corresponds to the positive selection for T-cell maturation.

Hussain *et al.* introduced this approach in order to mine unexpected rules (Hussain *et al*., 2000). Immature T-detector generation via unexpected rule mining is chosen since we believe that this method of implementation will provide self-MHC restriction of T-detectors, which concerns T-detector activation focus in the current self-context. This is because immature T-detectors are generated and selected based on currently presenting self-antigen information. In particular, we can find a direct resemblance between the elimination of immature T-detectors whose confidences are very low, and the removal of immature T-cells whose affinities are very weak during positive selection.

As shown in figure 3, immature T-detectors are then passed to the next process "Generate mature T-detectors". This process is analogous to negative selection of the HIS. During this process, immature T-detectors start being compared to two strong rules, which are comparable to self-MHC/peptide bindings. This process measures the distance between two strong rules and each immature T-detector. Then, as negative selection of the HIS only selects the T-cells with low affinities for self-MHC/peptide bindings, the process will select immature T-detectors whose distances to two strong rules are larger than a pre-defined threshold. The selected T-detectors now become mature T-detectors, which are ready for activation.

One thing that should be noted here is that the CIFD negative selection approach does not require T-detectors to avoid having high affinities with *all* self-MHC/peptide bindings. Instead, it only requires T-detectors to have low affinities with two strong association rules which have been used for generating immature T-detectors. After this modification, will mature T-detectors still have sufficient self-tolerance? To answer this question, it is necessary to understand how the T-detectors of CIFD activate. Since T-detectors exist as a form of "If-Then" rule, CIFD allows T-detectors to activate when any antigen, which is a transaction, is satisfied by the rule represented by a mature T-detector. That is to say that only a transaction which has attribute values described by the antecedent of a given mature T-detector can activate it. As seen above, the mature T-detector has been tolerant of all self-antigens that have attribute values of the T-detector rule antecedent. Therefore, mature T-detectors, generated as above, will still have adequate self-tolerance.

4.3 Self-MHC Diversity

Since self-MHC is a key molecule that determines mature T-cell activation, the diversity of self-MHC types strongly influences the overall immunity of the HIS (Hofmeyr, 2001). As the diversity of self-MHC types increases, there is a greater chance for non-self antigen peptides to bind self-MHC types. It is known that some viruses, such as the Epstein-Barr virus, evolved to avoid binding a certain type of self-MHC (Hofmeyr, 2001). As a result, individuals having this type of self-MHC are often found to be vulnerable to this virus.

Similarly, the T-detectors of CIFD would be more likely to bind diverse anomalies with varied self-MHC types. Currently, the self-MHC/peptide bindings of CIFD represented by association rules describe frequent patterns in transactions. However, there can be different sets of frequent transaction patterns depending on diverse time granularities. For instance, frequent transaction patterns in the morning of weekdays would be different from those in the evening at weekends. Thus, various types of self-MHC can represent various levels of frequent transaction patterns according to diverse time granularities.

To implement diverse types of self-MHC, CIFD uses calendar schema introduced by Li *et al.* (2002). A calendar schema is a relation schema, which represents a specific calendar category such as "for every morning of weekdays" or "for any time of Monday of the first week of the month". Li *et al.* modified *Apriori* so that it generates association rules according to various calendar schemas. This new algorithm mines an association rule such as "*If* milk *Then* bread with confidence = 50% for every Monday morning" or "*If* milk *Then* bread and Newspaper with confidence = 90% for every Saturday morning". Thus, all antigens presented to CIFD are represented according to different types of time granularity. As various types of self-MHC are more likely to bind diverse types of antigen peptides, the modified *Apriori* is more likely to generate diverse frequent transaction patterns within various time granularities.

5 CIFD Conceptual Architecture Overview

In this section, the conceptual architecture of CIFD is illustrated. CIFD includes six different processes that provide novel features introduced in sections 2 and 3 together with other features, which can be found from other AIS. The six processes are 1) Filter and Convert Transactions, 2) Self Profile, 3) Generate Detectors, 4) Apply Detectors, 5) Analyse Detections, and 6) Notify Detections. Figure 4 shows these processes.

The *Filter and Convert Transactions* process filters and converts input transaction data into a suitable format for processing by CIFD. Transaction data supplied to this study is extracted from a central system that handles daily

data from a large number of outlets operating within a retail business organisation. The retail business transaction data includes many attributes which do not need to be monitored for anomaly/fraud detection purposes. In addition, further information required for anomaly/fraud detection can be derived by converting existing attributes into new formats, e.g. "transaction time stamp" can be converted to "Day of Week" and "Time of Day".

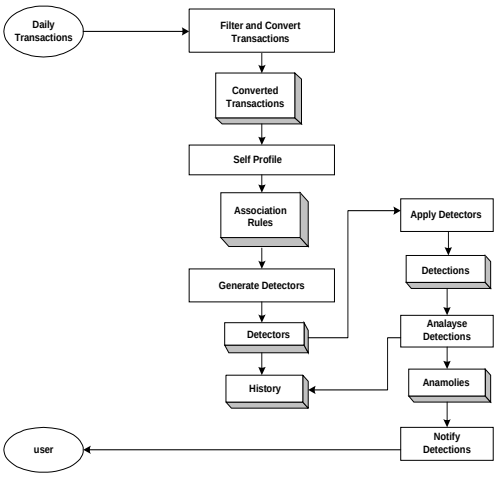

Figure 4. Conceptual Architecture of CIFD

The filtered and converted transaction data is passed to the *Self Profile* process. As discussed in the previous sections, CIFD requires a separate process to generate self-MHC/peptide bindings. The *Self Profile* process performs this task. It mines association rules, which describe frequent transaction patterns within various calendar categories.

The third process, *Generate Detectors*, generates three different types of detector: T-detectors, memory detectors and B-detectors. T-detectors play a similar role to that of T-cells of the HIS. T-detectors are generated through the T-detector maturation process introduced in section 4. In addition, immature detectors passed to the process "Generate Mature T-Detectors" in figure 3 have to be exposed to various self-MHC/peptide bindings over a specific timeframe before they become mature. This is because CIFD is designed to process one day's worth of data at one time, for overnight batch processing. Thus, a T-detector passing one negative selection test will be tolerant only over the given day's transactions. To ensure a T-detector is tolerant over a sufficient portion of self-antigens (at least all the antigens covering a calendar schema assigned to a T-detector), CIFD allows a T-detector to be mature only when it passes negative selection for a sufficient period.

Memory detectors perform the same role as memory cells in the HIS. Memory cells are replicas of T-detectors that are successful in detecting fraudulent transactions. As memory cells react to reappearing or structurally related antigens quicker than an initial reaction, so the CIFD memory detectors are also expected to detect similar anomalies/frauds to those detected previously.

B-detectors are analogous to the B-cells of the human immune system. In the human immune system, successful B-cells are cloned but with slight variations (Somatic Hypermutation) and thus they are expected to have associative antigen information. Similarly, the B-detectors in CIFD are generated by mutations of successful T-detectors[3]. The principal rationale behind the use of B-detectors is that there could well be new anomalies (potential frauds) that are committed by slightly modifying an existing anomaly/fraud scenario, and there may be yet other anomalies, which have similar points of vulnerability in common. These three different types of detector will exist as an "If-Then" rule form labelled by a specific calendar category. Furthermore, all detectors will have limited life spans so that they will be deleted after a while if they detect no anomaly. This feature means that CIFD dynamically learns fluid patterns in transactions.

The next process is the *Apply Detectors* process. All three types of detector are used to monitor new transaction data. When new transactions arrive, this process selects detectors whose calendar categories meet the time of the transactions. The selected detectors are simply compared to the transactions and filter the transactions that do not satisfy detector rules. The filtered transactions are sent to the *Analyse Detection* process with detectors for further analysis. The transactions detected by memory detectors may be passed to the *Analyse Detections* process immediately (this maps to a primary response of the HIS; Hofmeyr, 2001) whilst the other transactions detected by T and B-detectors may require detection by more than one detector to be passed to the *Analyse Detections* process (this corresponds to a secondary response of the HIS; Hofmeyr, 2001). This is one simple example of how CIFD would implement two different immune responses. However, more careful study is needed for actual implementation. For instance, the various confidence values of T-detectors may indicate different immune response thresholds, and B-detector may need help from T-detectors to trigger immune responses.

The *Analyse Detections* process analyses the transactions detected by the three different types of detector sets. Initial detection results need to be examined further in order to decide whether they are indeed anomalies. In the HIS, an additional confirmation signal called *costimulation* sent from the innate immune cells is required for immune cell activation (Kim, 2002; Hofmeyr, 2001). The role of costimulation is to disallow inaccurate reactions. In the same way, the CIFD system aims to allow human auditors to provide feedback into the system in order to lower the false positive rate in the future. A kind of visualisation tool would help auditors to analyse initial detection results. Auditors' analysis results will determine the detectors to be cloned and mutated to produce new B-

[3] It should be noted that this is a variation on the HIS. B-cells of the HIS are also matured in bone marrow and mature B-cells are released to the lymph nodes for activation. New B-cells generated by applying Somatic Hypermutation are on successful B-cells not T-cells.

detectors and memory detectors, in addition to CIFD's own contribution. In this case, auditors themselves can refine selected successful detectors in order to generate memory detectors and B-detectors. This mechanism would provide CIFD with the ability to learn. Therefore, we expect the degree of human intervention will decrease as CIFD learns more diverse anomaly/fraud types.

The *Notify Detections* process will notify the users of the final analysis of detection. It is important to present the final detection results of CIFD in a comprehensible format to the users. This should include some justification as to why CIFD detects some transactions as anomalous.

Among these six processes, the first two processes, the *Filter and Convert Transactions* and *Self Profile* are developed and tested. The details about these processes and test results are reported in (Kim, 2003).

6 Discussion and Related Work

In order to reduce the negative selection algorithm's computing time, several works have added an evolutionary approach. Ayara *et al*. (2002) introduced a modified negative selection algorithm by employing somatic hypermutation. To generate an immature detector, it selects a detector matching self-antigens and mutates the parts of the detector which match self-antigens. In addition, the mutation rate is determined proportionally to the affinity of the detector. The rationale behind this approach is the generation of mutants that are further away from self-antigens. Lamont *et al.* (1999) uses a genetic algorithm to generate detectors. The fitness function of a detector is defined as the growth rate of non-self space coverage by each detector. Dasgupta and Gozalez (2002) introduce a similar approach, employing a genetic algorithm to generate detectors. The fitness function reported there is defined as the growth rate of non-self space coverage by each detector with a penalty value, which is the number of matching self-antigens.

Work by Esponda, Forrest and Helman (2003) provides new theoretical analyses that show the number of detectors needed to maximise detection coverage when the algorithm uses negative selection and positive selection respectively. This work also estimates for the first time the self-set size that allows the negative selection algorithm to be computationally advantageous compared to positive selection. This work is significant because it allows evaluation of the feasibility of the negative selection algorithm before it is applied to a given problem. Another theoretical analysis by Wierzchon (2001) also introduces a new negative selection algorithm that requires low-space complexity to generate detectors.

All of these works use the negative selection algorithm for anomaly detection purposes such as network intrusion detection and fault detection. They have indeed shown better understanding of the negative selection algorithm and their modifications that might cure the scaling problem of the algorithm. Nevertheless, none of them has been tested on the huge volume of data that CIFD has to handle. From the above works, Lamont *et al* (1999) and Dasgupta and Gonzalez (2002) have tested their new systems on real data sets, whose sizes are 1.3Mbytes and unreported respectively. However, Lamont *et al* reported that their new suggestion requires far too much computation time to be applied to the given data set and Dasgupta and Gonzalez (2002) did not report computation time.

On the other hand, there are other AIS that process a large amount of real data for anomaly detection. Kephart *et al.* (1997) at the IBM research centre developed an AIS for virus detection and their prototype has eventually been developed into a commercial system (White *et al.*, 2000). Another AIS developed by Burgess (2000) is a proactive maintenance system for computer systems. Burgess (2000) puts the emphasis of AIS on an autonomous and distributed feedback and healing mechanism, triggered when a small amount of damage can be detected at an initial attacking stage.

Interestingly, these two research efforts deliver somewhat different messages from the other work introduced in this section. They attempt to identify and understand useful processes of the HIS, and to see how these can help with devising a new anomaly detection system. However, they do not attempt to implement the processes using the mechanism of the HIS, only to mimic it at a high level of abstraction. They advance other conventional algorithms to implement identified human immune processes. In other words, they treat each process of the human immune system as a black box and thus the actual implementation of this box is not considered important to provide the desired result from each process. This may have assisted them in building a commercially successful system. CIFD follows a similar philosophy. The relevance to the study of AIS is the understanding of useful immune mechanisms for FD, and the implementation of these mechanisms is not our main concern.

There are also other AIS that employ a mechanism analogous to self-MHC of the HIS. Forrest and Hofmeyr (2001) use a permutation mask as self-MHC, which defines a permutation of each detector binary string. As the diverse types of self-MHC present different types of peptides, the permutation mask allows multiple representations of detectors. Toma *et al.* (2000) used the internal state of mobile agents as self-MHC and the interaction with external information as self-MHC/peptide bindings. To the best of our knowledge, CIFD is the first AIS to employ self-MHC in order to provide a self-restriction feature and increase the diversity of detectors.

7 Conclusion and Future Work

This paper introduces a novel AIS, called CIFD (Computer Immune system for Fraud Detection) that is designed to scale to a huge volume of real data for fraud detection. In order to improve scalability, CIFD presents antigen data using an analogy of the self-MHC molecule

of the HIS. CIFD also employs negative selection combined with positive selection in order to reduce the computing time taken to generate T-detectors. Together with these novel features, CIFD is equipped with other immune features: i) adaptability, which allows CIFD to detect dynamically changing anomaly patterns and ii) the ability to learn, memorising previously detected anomaly patterns and quickly reacting to reappearing or structurally related antigens. These are implemented using rather well known artificial immune components such as clonal selection and memory detectors.

We also briefly study a group of AIS, which are designed to improve the scalability of the negative selection algorithm. The study shows that they have not been shown to scale to a large volume of real data yet, although they provide a better understanding of the algorithm and promising modifications. This group of work is then compared to the other group of AIS, which successfully scale to large amounts of real data. The interesting observation made from this comparison is that AIS's with good scalability treat each process of the human immune system as a black box and thus the actual implementation of this box is not considered important. This may have assisted them in building a commercially successful system. CIFD also follows a similar philosophy.

We are currently completing the development of *Filter and Convert Transactions* and *Self Profile* introduced in section 5. The preliminary test results are reported in (Kim, 2003) and thorough tests are currently being conducted. The results reported there show that CIFD successfully scales to 700 Mbyte data samples that contain a total of 5,054,878 transactions within an acceptable computing time. The detailed computation times taken for processing daily transactions are presented in (Kim, 2003). Whilst these results show promising first signs, it is necessary to test a completely developed CIFD if it is to be considered an effective anomaly detector. With this aim, the current work is focused on the development of positive and negative selection algorithms in the T-detector maturation process. The main research issues at this stage of work are i) devising an effective measurement that represents the distances between self-MCH/peptides bindings and an immature detector, ii) defining an appropriate tolerisation period for an immature detector and iii) defining a competent T-detector activation scheme.

Acknowledgments

This work is conducted as a LINK project under the auspices of the DTI Management of Information (MI) research programme.

Bibliography

Agrawal, R., and Srikant, R., (1994), "Fast Algorithms for Mining Association Rules", In *Proceeding of the 20th VLDB Conference*, Santiago, Chile, pp.487-499.

Ayara, M., *et al*., (2002), "Negative Selection: How to Generate Detectors", In Proceeding of the 1st Int. Conf. on AIS (ICARIS-2002), Canterbury, U.K., pp.89-98.

Burgess, M., (2000), "Evaluating Cfengine's Immunity Model of Site Maintenance", *Proceedings of the 2nd SANE system administration conference.*

Dasgupta, D., and Gozalez, F., (2002), "An Immunity-Based Techniques to Characterize Intrusion in Computer Network", *IEEE Transactions on Evolutionary Computation*, Vol 6., No.3, pp.1081-1088.

Lamont, G. B., *et al*., (1999) "A Distributed Architecture for a Self-Adaptive Computer Virus Immune System", *New Ideas in Optimization, Advanced Topics in Computer Science Series*, McGraw-Hill, London, pp, 167-183.

De Castro, L., N., and Timmis, J., (2002), *Artificial Immune Systems: A New Computational Intelligence Approach*, Springer-Verlag, London. UK., September 2002.

Esponda, F., Forrest, S., and Helman, P., "Positive and Negative Detection", *IEEE Transactions on Systems, Man and Cybernetics.* (in press).

Forrest, S., and Hofmeyr, S., A., (2001), "Immunology as Information Processing", *Design Principles for the Immune System and Other Distributed Autonomous Systems*, Segel, L. A., and Cohen, I., (Eds). Santa Fe Institute Studies in the Sciences of Complexity. New York: Oxford University Press, pp. 361 - 387.

Forrest, S., Hofmeyr, S., and Somayaji, A., (1997), "Computer Immunology", *Communication of the ACM*, Vol. 40, No.10, pp.88-96, 1997.

Hofmeyr, S., A., (2001), "An Interpretative Introduction to the Immune System", *Design Principles for the Immune System and Other Distributed Autonomous Systems*, Segel, L. A., and Cohen, I., (Eds). Santa Fe Institute Studies in the Sciences of Complexity. New York: Oxford University Press, pp. 3-26.

Hussain, F., Liu, H., Suzuki, E., and Lu, J., (2000), "Exception Rule Mining with a Relative Interestingness Measure", *Proc. of the Fourth Conf. PAKDD-00*, pp.86-97.

Kephart, J. O., *et al.*, (1997), "Biologically Inspired Defences against Computer Viruses", *Machine Learning and Data Mining: Method and Applications*, (Ed) Michalski, R. S., Bratko, I., and Kubat, M., John-Wiley & Son, pp.313-334, 1997

Kim, J., (2003), "Dynamic Temporal Rule Profiling using Calendar-based Association Rules: Application to Financial Fraud Detection in the Retail Sector", Technical Report, Dept of Computer Science, King's College London.

Kim, J. W., (2002), *Integrating Artificial Immune Algorithms for Intrusion Detection*, PhD Thesis, Department of Computer Science, University College London.

Kim, J., and Bentley, P. J., (2001), "Evaluating Negative Selection in an Artificial Immune System for Network Intrusion Detection", *Genetic and Evolutionary Computation Conference 2001 (GECCO-2001), San Francisco*, pp.1330 - 1337, July 7-11.

Lee, W., (1999), *A Data Mining Framework for Constructing Features and Models for Intrusion Detection Systems*, PhD Thesis, Department of Computer Science, Columbia University.

Li, Y., *et al*., (2002), "Discovering Calendar-based Temporal Association rules", *Journal of Data and Knowledge Engineering*, Vol. 44, No. 2, Elsevier, pp.193-218.

Sompayrac, L., (1999), *How the Immune System Works*, Blackwell Science Inc.

Tizard, I. R., (1995), *Immunology: Introduction*, 4th Ed, Saunders College Publishing.

White, S. R., *et al*., (2000), "Anatomy of a Commercial-Grade Immune System". http://www.research.ibm.com /antivirus/SciPapers.htm

Toma, N., *et al*., (2000), "The Immune Distributed Competitive Problem Solver with MHC and Immune Network", *Intelligent Engineering Systems through Artificial Neural Networks*, vol.10 (editor C.H. Dagli et al.), Asme Press Series, pp.317-322.

Wierzchon, S. T., (2001), "Deriving Concise Description of Non-Self Patterns in an Artificial Immune System", New Learning Paradigm in Soft Computing, Wierzchon, S. T., Jain, L. C., and Kacprzyk, J. (Eds.), Heidelberg, New York, Physica-Verlag, pp.438-458.

AAAI, (2002), "Fraud Detection and Prevention", http://www.aaai.org/AITopics/html/fraud.html