Using Clustering Techniques to Analyze Fraudulent Behavior Changes in Online Auctions

Wen-Hsi Chang/TamKang University
Graduate Institute of Management Sciences
Taipei, Taiwan
wenhsi.chang@gmail.com

Jau-Shien Chang/TamKang University
Department of Information Management
Taipei, Taiwan
jschang@mail.im.tku.edu.tw

***Abstract*—schemed fraudsters often flip behavior in terms of circumstances change as camouflage for disguising malicious actions in online auctions. For instance, the fake transaction records interwoven with real trades are indistinguishable from legitimate transaction histories. The ways of fraudulent behavior changes formulate different types of tricks for swindling. To avoid trading with fraudsters, recognizing the types of fraudulent behavior changes in advance is helpful in choosing appropriate trading partners. Therefore, in order to distinguish the types of behavior changes from different fraudsters, clustering techniques were applied such as X-Means for grouping in characteristics. Afterwards, C4.5 decision trees were employed for inducing the rules of the labeled clusters. In this study, the real transaction data of 236 proven fraudsters was collected from Yahoo!Taiwan for testing. The experimental results demonstrate that the fraudsters are categorized into 4 natural groups and the vast majority of fraudster, 93% of fraudsters on average, follows certain default models to develop a scam. The findings of this study also make online auction early fraud detection possible.**

Keywords- clustering; decision trees; e-commerce; fraud detection

I. INTRODUCTION

According to the statistics of Internet Crime Complaint Center in recent years, online auction fraud has been occupying a large of percentage [1]. Each schemed fraud was prepared by deliberate premeditation, not by coincidence. The preparation work of a fraud is a composite of behavior for appealing innocent buyers, such as raising reputation score. To keep away online auction fraud, recognizing the categories of fraud is helpful in choosing appropriate countermeasure against different fraudsters.

Originally, open information of transaction histories is useful to evaluate the credit level of a trading partner. However, those schemed fraudsters take it as a swindling tool to raise reputation for deceiving traders. Since schemed fraudsters are good at disguising malicious behavior and interleaving regular trades in their transaction histories, online auction fraud has become one of the most serious threats in Internet frauds [2]. For instance, they usually manipulate feedback score with different tricks for fabricating reputation. Notwithstanding their schemes for raising reputation score could be quite sophisticated, it is inevitable to leave some traits of committing a fraud in their transaction histories, such as the trend and magnitude of irregular behavior changes. This kind of abnormal behavior definitely reflects the results on the corresponding reputation management systems. Unfortunately, most traders could identify only part of fraudulent behavior without assistance from other information resources in usual. One of most popular solutions is to apply a fraud detection system that comprises known behavior patterns to inspect a suspicious account. Apparently, the kind of detection systems is only able to detect those fraudsters whose features of behavior exactly matched with existing behavior patterns. However, fraudsters often change their tricks in terms of current circumstances dynamically. As a consequence, even a minor modification for a trick could affect the accuracy of a fraud detection mechanism. Notwithstanding the changes of behavior cause fraud detection harder, the fraudulent behavior still follows certain models or types in most cases of fraud. It is impossible to make a detection mechanism has zero misclassification as expected as a new upcoming trick.

Therefore, we take the types of tricks for committing a fraud into account to categorize fraudulent behavior into natural groups in characteristics by clustering techniques. Afterwards, to identify a minor modification of a trick, the similarities to existing fraudulent patterns were calculated to enhance the effectiveness of fraud detection.

In this study, we employ X-means algorithm, which is an extended K-means clustering technique to categorize 236 proven fraudsters in Yahoo!Taiwan into 4 types. In addition, C4.5 algorithm was applied for explaining the rules of the labeled fraudulent behaviors respectively.

The rest of this article is organized as follows: Section 2 is related work on types of anomalies, measuring attributes in online auctions, and clustering techniques we applied. The third section is to discuss the behavior changes from our observations. Section 4 presents fraudster clusters in nature. The experimental results are presented in the section 5. Finally, conclusions and future research directions are mentioned in the last section.

II. RELATED WORK

In the real world, there are merely very few auction fraudsters among the vast majority of legitimate accounts. That is, a fraudster is anomaly in online auctions. Therefore, online auction fraudster detection refers to the problem of finding fraudulent behavior patterns in transaction histories. In other words, online auction fraud detection is one of applications of anomaly detection. The capability of identifying anomalies determines the effectiveness of a fraud detection system. For instance, Rubin proposes a new

978-1-4244-7578-0/$26.00 © 2010 IEEE

reputation system to help buyers identify anomalies in online auctions such as sellers whose auctions seem price-inflated etc. [3].

A. Types of Anomalies

The key components of anomaly detection are in associated with anomaly detection techniques including the nature of the data, availability of labeled data, and type of anomalies to be detected. In addition, anomalies can be categorized into following 3 types [4]:

1) *Point Anomalies*
2) *Contextual Anomalies*
3) *Collective Anomalies*

Such as a credit card fraud defined only amount spent is a classic point anomaly. If a transaction were higher than the normal range of expediture for that person, it could be a fraud. Similar situations often occur in online auctions, traders usually estimate corresponding trading partners only with accumulated negative ratings.

According to our observations, a schemed fraud could be a contextual anomaly. Contextual anomalies refer to an instance is anomalous in a specific condition, but not otherwise. The context of an instance is a part of fraud formulation. For instance, the more positive ratings a trading participant got the higher reputation he has. However, the context of a fraud is the high density of obtaining positive ratings, which implies reputation inflation. Therefore, each case of fraud should be defined by contextual attributrtes and behavior attributes.

Not only can a fraudster activate a fraud, but also a group of accounts as well such as an accomplice syndicate. However, not all members of the syndicate committed the fraud, and most of them look like legitimate accounts individually. As the collection of related instances is anomalous with respect to the entire data set is a collective anomaly. The three types of anomalies could be presented in online auctions in general.

B. Measuring Attributes

A set of appropriate measuring attributes can depict the features of a fraudster precisely for building behavior models. To observe the behavior changes of a fraudster, first and foremost is to determine which measuring attributes are applied to describe fraudulent behavior. Chau and Faloutsos defined 17 price-oriented attributes for detecting fraudsters in online auctions [5] that includes median prices of items sold, median prices of items bought, standard deviation of the prices of items sold, standard deviation of the prices of items bought within the first 15, first 30, last 30, and last 15 days in transaction history. In addition, the ratio of the number of items bought to that of all transactions. The 17 measuring attributes could depict point anomalies and part of contextual anomalies with statistic values.

To enhance the capability of depicting contextual anomalies, Chang and Chang defined another 7 measuring attributes as follows [8]:

1) *Density of obtaining positive ratings*
2) *Density of obtaining negative ratings*
3) *Density of obtaining positive ratings after closing bid*
4) *Given being a seller, the ratio of positive ratings from other sellers to all positive ratings*
5) *Time difference from the last negative rating to the current time*
6) *Ratio of positive ratings to total feedback count*
7) *Ratio of negative ratings to total feedback*

The combination of the two sets of measuring attributes above that includes behavior attributes, statistic attributes and particular values was proven effective in online auction fraudster detection in previous experiments.

C. Clustering Techniques

Clustering is a simple and straightforward technique to partition instances into disjoint groups [9]. K-means is one of the classic clustering techniques using an iterative distance-based algorithm. In advance, the number of clusters should be determined by the parameter *k*. Then the algorithm randomly chooses *k* points as cluster centers. Subsequently, each instance is assigned into its closest center by Euclidean distance function, as finding the nearest neighbors. And then the mean of distances in each cluster will be calculated as new center values for each cluster. That is, each iteration process produces a set of cluster centers and all instances must be examined and assigned to the nearest center. Iteration processes will be continued until the same points are assigned to each cluster centers has stabilized and will remain the same forever [7].

In following experiments, we apply X-Means instead, which is an extended version of K-means clustering technique in structure implemented by Weka 3.7.0, to analyze behavior changes of online auction fraudsters who are divided into natural groups by characteristics rather than default classes. X-Means improves the computation for searching the space of cluster locations and number clusters to optimize the Bayesian Information Criterion (BIC) measure. It attempts to split the center in its region. X-Means compares the BIC-values of the two structures between the children of each center and itself to make decision [8].

III. Behavior of Fraudsters

A. Earlier-Phased Behavior Simulation

A premeditated scam is a sophisticated composite of behavior changes along with different tricks. According to our observations, there always is a certain break point between activating a fraud and its preparation work. In general, the descriptive value of each measuring attribute reflects the level of current situation or behavior status only. Therefore, it is difficult to identify a fraudster who fabricates feedback score as camouflage with bare eyes, especially before a fraud being activated.

To simulate the processes of fraudulent preparation work, we extract part of the transaction histories for monitoring easily. To look backward the earlier stages of a fraudster, cut the last part of transaction history off is a simple and straight approach for simulation. Thus, a phased partitioning method

was developed for simulating the behavior in the earlier phases. The transaction history of a proven fraudster was suspended or voided is treated as a complete lifespan. Hence, we used the percentage of a transaction history to indicate the earlier phases for preparation work.

Both the count of ratings and the duration of being at the site could present the lifespan of a fraudster. In addition, a transaction history consists of information about positive ratings and negative ratings mainly. Hence, Chang and Chang proposed a method for partitioning transaction histories as follows [6]: The length of a transaction history equals to the count of accumulated ratings. Thus, given an account u and its transaction history $TH(u)= \{tr_1, tr_2, \cdots, tr_n\}$, the r% lifespan of u is denoted as $TH(u, r\%)=\{tr_1, tr_2, \cdots, tr_d\}$, and $d=\lceil n*r\% \rceil$. The r% of transaction history indicates the r% earlier stage of its lifespan. For example, if n=60, then $TH(u, 80\%)$ would be $\{ tr_1, tr_2, \cdots, tr_{48} \}$(See Fig. 1)

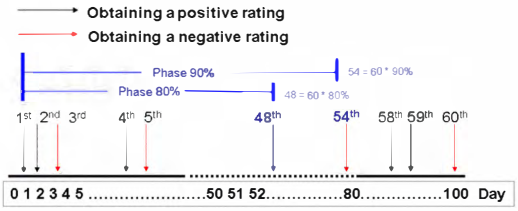

Figure 1. Phased partition of transaction history

B. *Difficulites of Fraudulent Behavior Detection*

There are several challenges and difficulties of online auction fraud detection as follows:

1) The boundary between normal and anomalous behavior is often not precise

2) In online auctions, fraudulent behavior keeps evolving and stable patterns might not sufficiently depict fraudsters.

3) Sometimes a small deviation from legitimate accounts might be an anomaly, but some fluctuations in the trading behavior might be considered as normal.

4) It is very difficult to distinguish the behavior of a normal account containing noise data is simliar to actual anomalies.

To resolve the problems above, we adopt a composite of measuring attributes that includes statistic values, particular values, and contextual values for depicting fraudulent features from different aspects. We use some statistic value as measuring attributes to take the advantage of controlling small deviation. In particular, we emphasize the contextual situation description in following experiments for compensating the ambiguity between normal and abnormal behavior. Therefore, some particular values were introduced for indicating certain contextual situations. To overcome these difficulties above, the method of partitioning transaction histories is integrated with previous measured attributes for emulating the preparation status of a fraudster, the latency period.

IV. FRAUDSTER CLUSTERS

There are different ways in which the result of clustering can be expressed [7](See Fig. 2). The presentation of clustering should be dictated by the nature of the problem that is thought to underlie the particular situation. Thus, fraudulent behavior may be categorized into exclusive or overlapping clusters. Moreover, it is possible to have these clusters in hierarchical or partial hierarchical structure. For instance, it could be a crude division of instances at top level. Or the clusters are identified probilistic, whereby and instance belongs to each group with a certain probability.

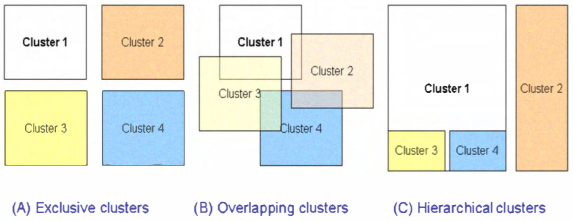

Figure 2. Different presentation of clusters

Behavior fluctuation between regularity and irregularity is a common trick for schemed fraudsters. The features in the different phases of a latency period could be clustered into different clusters for pragmatic reasons. The following experiments are to discover the types of fraudulent behavior changes via clustering.

V. EXPERIMENTAL RESULTS AND ANALYSES

We collected the real transaction histories of 236 proven fraudsters from the blacklist of Yahoo!Taiwan. The transaction history of each fraudster was partitioned into 5 different phases based on the count of accumulated ratings, such as phase 100%, 95%, 90%, 85% and 80%, as Fig. 1 illustrates. Each specific phased profile contains 24 numeric values by the proposed composite of measuring attributes. As a result, the data set consists of 1,180 phased profiles for testing. The experimental results explain that most fraudsters followed specific formulations to change behavior.

A. *Results of Clustering by Mixed Phased Profiles*

Table 1 shows the experimental results of applying X-Means algorithm, in which the total 1,180 fraudulent profiles are categorized into 4 clusters. The 4 clusters indicate the nature of online auction fraudsters in characteristics, which are respectively labeled by type 0, type 1, type 3 and type 4. Type 2 is the most popular type of fraud that occupied 39% of online auction fraudsters. Type 0 occupied 31%, type 1 is 21% and only 9% of fraudsters belong to type 3. The rest of them were shown in Table1.

TABLE I. RESULTS OF CLUSTERING

	Type 0	**Type 1**	**Type 2**	**Type 3**
Phase100%	72	51	93	20
Phase 95%	73	50	93	20
Phase 90%	72	51	91	22

Phase 85%	73	50	90	23
Phase 80%	73	49	91	23
Total	363	251	458	108
***Percentage**	31%	21%	39%	9%

* The percentage for each individual type of fraudulent behavior being occupied

According the statistics of Table 2, almost all different phased profiles of an account have been assigned into the same cluster. Performing continuous tests to a suspect before he has been suspended would be helpful in identifying to which type of fraudster he belongs. 96% of Type 0 fraudsters could be identified into the same type whether their current phases are. The rest of types presents similar results, 92% of Type 1, 96% of Type 2 and 87% of Type 3 could be identified in all 5 phases. Averagely, 93% of fraudsters will follow the same model to develop their schemes during the entire lifespan. The results denote the behavior of most fraudsters might be detected as early as possible.

TABLE II. THE COUNTS OF BEING IDENTIFIED BY PHASED PROFILES

Phases	**1**	**2**	**3**	**4**	**5**	***Percentage**	**Average**
Type 0	0	2	0	1	71	96%	93%
Type 1	1	0	2	1	48	92%	
Type 2	1	2	1	0	90	96%	
Type 3	0	1	2	0	20	87%	

*The percentage of the type of fraudsters can be categorized into the same type in all 5 phases

According to the experimental results, most fraudsters will keep following a type of model in general. Fig. 3 shows that general fraudulent behavior develops linearly with respect to phase progress.

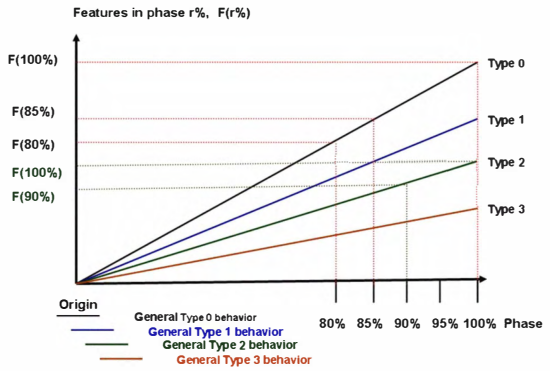

Figure 3. General Fraudulent Behavior Development

Some cunning fraudsters' behavior may not always keep stable to develop with respect to the same model as expected. In addition, even a regular legitimate account sometimes will change their purchase habits instantly as well under certain circumstances.

B. *Early Fraud Detection*

Since the experimental results above indicate that the X-Means clustering algorithm could identify a fraudster in the earlier phases before the time of being suspended (Phase 100%), it makes early online fraud detection possible.

To discover the implications of different types, C4.5 decision trees were employed with 10 folds cross validation to induce rules as follows:

```
DensityOfNeg <= 0.633333
| RatioOfBuyingRate <= 0.333333
| | MdSellingFirst15 <= 11150
| | | DensityOfNeg <= 0.541667: Type1
| | | DensityOfNeg > 0.541667
| | | | MdSellingFirst15 <= 2570: Type1
| | | | MdSellingFirst15 > 2570: Type0
| | MdSellingFirst15 > 11150: Type0
| RatioOfBuyingRate > 0.333333
| | RatioOfBuyingRate <= 0.375
| | | MdBuyingFirst15 <= 900: Type1
| | | MdBuyingFirst15 > 900: Type3
| | RatioOfBuyingRate > 0.375: Type3
DensityOfNeg > 0.633333
| RatioOfBuyingRate <= 0.190476
| | StdBuyingFirst15 <= 7.545694: Type0
| | StdBuyingFirst15 > 7.545694
| | | MdBuyingFirst15 <= 305: Type2
| | | MdBuyingFirst15 > 305: Type0
| RatioOfBuyingRate > 0.190476
| | MdSellingFirst30 <= 9300
| | | StdSellingFirst15 <= 238.5
| | | | StdBuyingFirst30 <= 1341.155721
| | | | | StdSellingLast15 <= 6320.551796
| | | | | | StdBuyingLast30 <= 755.323698: Type2
| | | | | | StdBuyingLast30 > 755.323698
| | | | | | | DensityOfNeg <= 0.804878: Type3
| | | | | | | DensityOfNeg > 0.804878: Type2
| | | | | StdSellingLast15 > 6320.551796
| | | | | | MdBuyingFirst15 <= 450: Type0
| | | | | | MdBuyingFirst15 > 450: Type2
| | | | StdBuyingFirst30 > 1341.155721
| | | | | MdBuyingFirst15 <= 3050: Type3
| | | | | MdBuyingFirst15 > 3050: Type2
| | | StdSellingFirst15 > 238.5
| | | | MdSellingLast15 <= 11400: Type3
| | | | MdSellingLast15 > 11400: Type2
| | MdSellingFirst30 > 9300: Type0
```

We scrutinize the above rules, most Type 2 and Type 3 fraudsters got higher density of obtaining negative ratings, and the prices of purchased commodities are lower on average. They might raise credit by purchasing the items with smaller amount money. On the contrary, Type 0 and Type 1 of fraudsters got lower density of obtaining negative ratings, and the higher prices of purchased goods.

Type 0 is traditional premeditated fraudster who got very high density of obtaining positive ratings for raising credit score in very short period. Type 3 could be a kind of very cunning schemed fraudster who used to flip behavior to appeal targets. All 1,180 profiles were labeled by the results of clustering; the averaged recall rate is 98.6% (see Table 3).

TABLE III. OUTCOME OF APPLYING C4.5 DECISION TREES

TP Rate	**FP Rate**	**Precision**	**Recall**	**F-Measure**	**Class**
0.989	0.006	0.986	0.989	0.988	Type 0
0.984	0.002	0.992	0.984	0.988	Type 1
0.989	0.007	0.989	0.989	0.989	Type 2
0.972	0.004	0.963	0.972	0.968	Type 3

Table 4 shows that prediction errors occurred in the previous experiment by C4.5. The results demonstrate that Type 0 and Type 3 are exclusive, but Type 0 might be misidentified as Type 1 or Type 2. Type 1 could only be misidentified as Type3, neither the other types. Type 2 and Type 1 are exclusive too. It is more difficult to identify Type fraudster by clustering.

TABLE IV. PREDICTION ERRORS

	Type 0	Type 1	Type 2	Type 3
* Type 0			X	
* Type 1	X			X
* Type 2	X			X
* Type 3		X	X	

*Predicted class; X denotes incorrect predicted class

C. *Changes of Fraudulent Behavior*

Referring to Table 5, there are 7 of the 236 fraudsters who switch their behavior into different types during the entire lifespan. The 7 instances indicate the phenomenon of overlapping clusters in Section 4. Table 5 also explains why the changes of fraudulent behavior affect the accuracy of clustering.

TABLE V. FRAUDULENT BEHAVIOR SWITHING PATTERNS

Fraudster	A1	A2	A3	A4	A5	A6	A7
Phase 100%	Type 1	Type 0	Type 1	Type 1	Type 2	Type 2	Type 2
Phase 95%	Type 1	Type 0	Type 0	Type 1	Type 2	Type 2	Type 2
Phase 90%	Type 1	Type 1	Type 0	Type 1	Type 3	Type 3	Type 2
Phase 85%	Type 0	Type 1	Type 0	Type 1	Type 3	Type 3	Type 3
Phase 80%	Type 0	Type 1	Type 0	Type 2	Type 3	Type 3	Type 3

We listed the results of clustering for analyzing in details. There are 3 kinds of behavior switching patterns between types that include Type 0 and Type 1, Type 1 and Type 2, and Type 2 and Type3. Whereas, Type 0 and Type 3 are mutually exclusive as follows:

1) *Type 0 and Type 1: Fraudster A1, A2, A3*
2) *Type 1 and Type 2: Fraudster A4*
3) *Type 2 and Type 3: Fraudster A5, A6, A7*

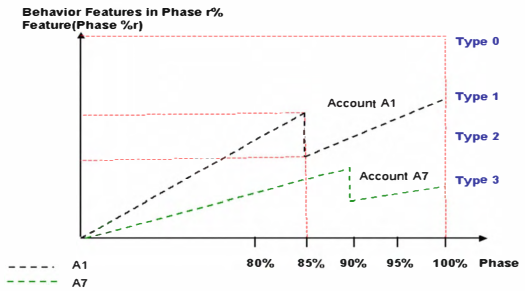

Figure 4. 2 Examples of fraudulent behavior switching

Fig. 4 shows account A1 and A2 didn't follow the default models linearly with respect to corresponding phases. Fraudster A1 develops his scheme in phase 80%-85% as Type 0, and then he changes his behavior into Type 1 when he steps into phase 90%. Account A7 originally develops his scheme as Type 2, whereas he turned his scheme into Type 3 at the point of phase 90%.

VI. CONCLUSIONS AND FUTURE WORK

Fraudulent behavior changes have been perplexing the construction of fraudulent behavior models. The experimental results show that applying clustering techniques to categorize fraudulent behavior into natural groups is helpful in discovering fraudsters as early as possible. In spite of which kind of tricks fraudsters apply, the vast majority of fraudster will still follow certain models to develop scams in general. In other words, this finding infers that fraudster could be identified in their earlier phases, even in phase 80%.

The similarity metrics of clustering techniques are similar to instance-based learning classification methods. In clustering, it groups different behavior in which all instances are processed altogether, whereas applying instance-based learning algorithm of which test instances are calculated individually. Therefore, the results of clustering could be applied to label outcome classes for enhancing the functionality of a supervised classification method. Hence, we are going to apply different instance-based learning algorithms to identify fraudulent behavior as the future research directions. In addition, hierarchical cluster analyses could be conducted to refine fraudulent behavior changes in details for further applications.

REFERENCES

[1] National White Collar Crime and the Federal Bureau Investigation, "2009 Internet Crime Report", Mar. 2010, pp.1-28, http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

[2] B. Gavish and C. L. Tucci, "Reducing Internet Auction Fraud., Commun. ACM, vol. 51, no. 5, May. 2008, pp. 89-97. doi:10.1145/1342327.1342343

[3] S. Rubin, M. Christodorescu, V. Ganapathy, J. T. Giffin, L. Kruger, , H. Wang and N. Kidd, "An auctioning reputation system based on anomaly," In Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS 05), Alexandria, VA, USA, Nov. 7- 11, 2005, pp. 270-279.

[4] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Comput. Surv. vol. 41, no.3, Jul. 2009, pp. 1-58, doi:10.1145/1541880.1541882

[5] D. H. Chau and C. Faloutsos, "Fraud Detection in Electronic Auction," in Proceedings of European Web Mining Forum (EWMF 2005) at ECML/PKDD, Oct. 3-7, 2005

[6] J. S Chang and W. H. Chang, "An Early Fraud Detection Mechanism for Online Auctions Based on Phased Modeling," In Proceedings of The 2009 International Workshop on Mobile Systems, E-commerce and Agent Technology (MSEAT2009), Taipei, Taiwan, Dec. 3-5, 2009

[7] I. H. Witten and E. Frank, "Data mining: Practical machine learning tools and techniques", San Francisco: Morgan Kaufmann, 2005, pp. 136-139

[8] D. Pelleg and A. W. Moore, "X-means: Extending K-means with Efficient Estimation of the Number of Clusters," In Proceedings of the Seventeenth international Conference on Machine Learning, June 29 - July 02, 2000, P. Langley, Ed. Morgan Kaufmann Publishers, San Francisco, CA, 2000, pp. 727-73