A Game-Theoretic Approach to Credit Card Fraud Detection

Vishal Vatsa[1], Shamik Sural[2], and A.K. Majumdar[1]

[1] Department of Computer Science & Engineering
[2] School of Information Technology,
Indian Institute of Technology, Kharagpur, India
vishalvats@yahoo.com, {shamik@sit, akmj@cse}.iitkgp.ernet.in

Abstract. Intrusion prevention mechanisms are largely insufficient for protection of databases against Information Warfare attacks by authorized users and has drawn interest towards intrusion detection. We visualize the conflicting motives between an attacker and a detection system as a multi-stage game between two players, each trying to maximize his payoff. We consider the specific application of credit card fraud detection and propose a fraud detection system based on a game-theoretic approach. Not only is this approach novel in the domain of Information Warfare, but also it improvises over existing rule-based systems by predicting the next move of the fraudster and learning at each step.

1 Introduction

Intrusion detection is a critical part of the measures implemented for maintaining an attack tolerant database system. Though database management systems can provide intrusion prevention up to a certain extent by virtue of traditional access control mechanisms, they would not be sufficient for protection against syntactically correct but semantically damaging transactions [1]. Chung et al bring out that misuse detection in database systems has not been adequately addressed and propose DEMIDS, which can derive user profiles from database audit logs [2]. Lee et al suggest tagging the data objects with "time semantics" and monitor behavior at the level of sensor transactions [3]. Hu and Panda concentrate on analyzing the dependencies among data items in a database [4].

Consider a database system in an organization and a set of authorized users who have access rights on the database such as in banking services, credit card companies,etc. There always exists the possibility of legitimate and even non-legitimate transactions, what we hereby term as *fraudulent transactions*, being attempted by the authorized users or more typically, by adversaries posing as authorized users. The primary objective of any defense mechanism monitoring such an application would be to identify these fraudulent transactions as early as possible while limiting the possibility of raising too many false alarms. This form of Intrusion Detection in databases is an essential component of Information Warfare. The situation can be visualized as two adversaries playing against each other, the attacker launching attacks against the database system and the

S. Jajodia and C. Mazumdar (Eds.): ICISS 2005, LNCS 3803, pp. 263–276, 2005.

detection system countering it. The problem effectively models as a typical game with each player trying to outdo the other and Game theory has long been used to tackle such problems.

The field of Game theory has been explored for problems ranging from auctions to chess and its application to the domain of Information Warfare seems promising. Samuel et al bring out the role of Game theory in Information Warfare [5]. They highlight that one can utilize well-developed Game theory algorithms to predict future attacks and the differences and challenges in this domain as compared to traditional games like chess, such as limited examples, multiple simultaneous moves and no time constraints [6]. Liu and Li have presented a game-theoretic attack prediction model for attacks on IDS-protected systems [7]. The authors have considered choosing a threshold by the detection system dependent on the profile of the customer and the availability weight provided by the system. It is clear that if the threshold is low, it may result in the genuine transactions being rejected causing a negative payoff to the cardholder, which is considered as zero by the authors. Further, in a real-world scenario, the genuine cardholder cannot be expected to choose his action according to Nash Equilibrium and any deviations can only be suspected. As the detection system increases the availability weight, to avoid denial of service to the customer, there is no pure strategy equilibrium and the thief can act to maximize his payoff. Our model is not limited by these assumptions and we also improvise by including the possibility of 'learning' in our system, which takes place at every step of the multi-stage game. This was also validated by our experimental study.

The rest of the paper is organized as follows. Section 2 describes the work related to credit card fraud detection. Section 3 describes the Game-theoretic model and the architecture of the proposed fraud detection system (FDS). In Section 4, we describe the experiment conducted and analyze the results. We conclude in Section 5 of the paper.

2 Related Work

Fraud, as in the Encyclopedia, is defined as "willful misrepresentation intended to deprive another of some right" and is a major source of concern in a number of applications such as e-commerce, telecommunication industry, computer intrusion, etc. Credit card fraud is a growing problem in the credit card industry. In the USA, the online retail sales were reported to be $ 144 billion in 2004, which was a 26% increase over 2003 [8]. It is also estimated that 87% of purchases made over the Internet are paid by credit card [9]. The Association of Payment and Clearing Services (APACS) report showed that the cost of credit card fraud reached $ 966.74 million in 2004, which was an increase of 20% as compared to 2003 [10]. Another survey of over 160 companies revealed that online fraud (committed over the Web or phone shopping) is 12 times higher than offline fraud (committed by using a stolen physical card) [11]. The growing number of credit card users worldwide provides more opportuni-

ties for "thieves" to steal credit card details and subsequently commit fraud. A notion that rule-based systems, which take into account attributes like shipping address, product type, IP address, etc, should suffice for fraud prevention would be misleading. Labeling any transaction as 'fraudulent' is difficult for any static rule-based FDS due to a variety of reasons such as orders being shipped to an address different from billing address, genuine orders consisting of sale-able items like jewelry, etc. Confirming every suspected transaction from the genuine cardholder is not always possible or even practical due to the cost factor involved.

Though there are a variety of ways in which credit card fraud can be perpetrated, we classify them into two broad categories. This brings out the difference in the way frauds are carried out and also in the detection techniques used against them.

Physical Card. The cardholder either loses the card or his card is stolen and is then used by somebody else. This is the most fundamental type of fraud. In this case a substantial financial loss would occur only if the cardholder does not realize the loss of his card. Intuitively, the fraudster would attempt large volume or large value purchases in the shortest possible time. This should not be too difficult to detect by the fraud detection system in place.

Virtual Card. The second type of fraud, which is more difficult to tackle, can take place if the cardholder does not realize that someone else is in possession of his card details. This would also encompass the fraud that takes place due to counterfeit cards. These kinds of frauds may or may not get noticed, which depends on the strength of the fraud detection system in place. Further, the genuine cardholder in this case, will be able to detect the fraudulent transactions on his card only when he receives the credit statement at the end of the month.

Some of the common ways by which a fraudster can obtain the credit card details of an unsuspecting cardholder are shoulder surfing, dumpster diving, packet intercepting and database stealing [12]. We also add that unscrupulous employees at merchant establishments, restaurants, gas stations, etc, can note credit card details and possibly pass them on to an organized group of fraudsters. A variety of secure payment systems have been proposed to thwart credit card fraud such as Address Verification Service (AVS), Card Verification Value, Secure Electronic Transactions (SET) protocol, Secure Socket Layer (SSL), etc [13]. Even if we disregard the problems that may be peculiar to a particular payment system, it may be noted that in general, they will be ineffective against shoulder surfing, dumpster diving and database stealing, where the credit card details are known to the fraudster.

Credit card fraud detection has drawn lot of interest and a number of techniques, with special emphasis on data mining and neural networks, have been proposed to counter fraud in this field. Low et al described a method to implement a credit card system that would protect person's identity using simple cryptographic blocks [14]. Ghosh and Reilly carried out a feasibility study for Mellon

Bank to determine the effectiveness of neural network for credit card fraud detection [15]. The neural network used for this study is the P-RCE (Restricted Coulomb Energy) neural network. The authors concluded that it was possible to achieve a reduction of 20% to 40% in the total fraud losses. Aleskerov et al presented CARDWATCH, a database mining system based on a neural network learning module [16] . The system trains a neural network with the past data of a particular customer, which can then be used to process the current spending behavior and detect anomalies and they assume that since the normal behavior of the thief is to purchase as much as possible in limited time, the anomaly in transactions will most probably be detected. Chan et al divide a large data set of transactions into smaller subsets and then apply the mining techniques in parallel in a distributed data mining approach [17]. The resultant base models are then combined to generate a meta-classifier. More recently, Syeda et al have discussed the use of parallel granular neural networks for fast credit card fraud detection [18]. The parallel granular neural network (GNN) aims at speeding up the data mining and knowledge discovery process. The above-mentioned techniques, in general, attempt to either train a neural network with training data and then classify fraudulent/legitimate transactions or detect anomalies from the large amount of data using data mining techniques. These approaches would largely be static in nature and hence, would suffer from the limitation that the methodology being employed can be figured out by the fraudster. In contrast, we present a Game-theoretic approach for credit card fraud detection and propose the model of a FDS. The FDS improvises by using Game-theoretic techniques for fraud detection in addition to the existing ones and learns at each step of the game. This enables the FDS to predict the next move of the fraudster and switch to a counter- strategy at any stage to minimize the opponent's payoff.

3 Proposed Fraud Detection System

The proposed FDS is modeled with a two-tiered architecture. We aim at including some of the useful features available in commercial Fraud Detection systems while we improve upon it by including a layer working on Game-theoretic strategies. In our proposed system, the first line of defense is an intelligent rule-based system while the second uses Game-theoretic techniques for fraud detection. It may be noted that though we have considered transaction amount as an attribute for prediction, any other feature such as 'duration between transactions' can also be similarly considered.

3.1 Game-Theoretic Model

The presence of *two parties with conflicting goals* provided us with the initial impetus to use Game theory as an approach for fraud detection. In our quest to develop a Game-theoretic model for credit card fraud detection, the problem was compared with some well-known games such as "Bridges Problem", "D-day game"

and "Inspection Game" to find similarity and differences in comparison. Our initial motivation was the classic "Bridges Problem" [19] . It is safe to assume that the fraudster is likely to have a pre-conceived notion about the system trying to judge transactions based, at least, on the amount range. The fraudster, hence, faces the option of choosing between two, three or more bridges (depending on the ranges), each associated with a certain amount of risk. The problem also draws similarity to the D-day game, which is a situation involving the Invasion of France during World War II [20]. The game involves the Allies and Germany, with three possible sites for the Allies to invade. In order to win, the Allies need to choose a site where the Germans are not expecting them. Another possible model is that of the Inspection Game between a customs inspector and a smuggler [21]. The Inspection Game is played in n stages wherein the smuggler may choose one of the stages to attempt an illegal act. Murali and Laxman proposed detecting network intrusions via sampling with a game-theoretic approach [22]. The problem requires detecting an intruding packet in a communication network and has been modeled as a two-person zero-sum game.

We realized subtle differences these games had when compared to the situation we intended to work upon. For example, in the Bridges Problem, the thief is aware about the risks/uncertainty associated with a bridge while we would have to consider the risks to be implicit. Further, the thief is unaware about the ranges specified by the IDS and also, he may be working with completely different payoffs as compared to those assumed by IDS. Assumptions like, the smuggler learns of each inspection as it is made or that the inspector may announce his mixed strategy would be too weak in the case of fraud detection [23]. The study of these games and a variety of others helped us in devising a new model for the credit card detection system and introducing some strategies in our experimental setup.

We model the situation as a game between two players, the thief and the FDS. As stated earlier, it is safe to assume that the thief is likely to attempt a fraudulent transaction with a belief that his transaction may be monitored on the basis of transaction amount. For example, a very high value transaction is likely to raise an alarm. Hence, the aim of the thief is to avoid suspicion/detection by the FDS and try to maximize his payoff, either in the long run or in a short time (for fear of the fraud being detected before long). On the other hand, the aim of the FDS is to minimize its loss by detecting the fraud at an early stage. In our model, the loss can be minimized if the system is able to predict the next move of the thief correctly. In such a scenario, we say that the thief has been 'caught'. The dilemma for the thief, on the other side, is to be able to choose a transaction range that has not been predicted by the FDS.

The game, in case of three transaction ranges, can be modeled as shown in Figure 1. The thief, oblivious of the ranges or the strategies used by the FDS, needs to choose the ith range from the possible 'n' ranges. The FDS, in contrast, is unaware of the thief's choice and hence, the possible choices form the information set for the FDS. A correct prediction of the ith range by the FDS results in the thief being caught.

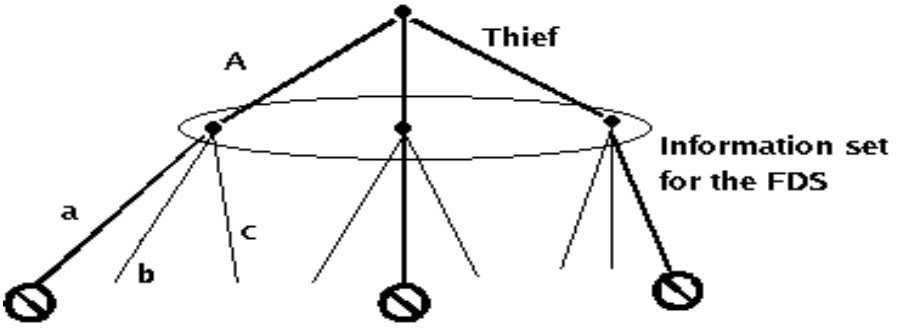


Fig. 1. Modeling the game

3.2 Architecture

The Fraud Detection System comprises of two layers, the 'Rule-based component' and the 'Game-theoretic component'. We discuss the two components separately.

The First Layer. We felt the necessity of the first layer not only for inclusion of certain features from available systems but also because we do not want to tackle millions of transactions with the Game theory rules, most of which are carried out due to routine use of credit cards. This layer would have rules like average daily/ monthly buying, shipping address being different from billing address, etc. In addition, customer-specific rules can also be incorporated. Intuitively, the first layer can filter out seemingly genuine transactions as is being done by the existing systems.

In an application such as credit card fraud detection, it is very difficult to conclusively declare that a given transaction is fraudulent. One may initially only suspect a transaction to be fraudulent with a certain probability. Consider the most basic of the checks which is used in many of the commercial systems and by various credit card companies, namely, billing and shipping address mismatch. However, such a mismatch could be either due to a fraudster aiming to get items delivered at an address or the actual cardholder gifting an item to a friend. In view of this, the First Layer of our proposed architecture uses generic as well as customer-specific rules to calculate the overall suspicion score for a transaction that is submitted. To amplify the idea, consider assigning weights to the different attributes of a transaction or better still, to a series of transactions on the same card number. Transactions scoring high due to attributes such as 'high value', 'sale-able item', 'address mismatch', etc, may trigger an alarm albeit the possibility of it being false cannot be ruled out. The main idea is that given a transaction and a specific user, what confidence measure can be assigned for the transaction to be from the genuine cardholder. Hence, the First Layer flags a transaction as 'suspect' if it crosses a user-defined threshold level. This introduces a trade-off between false positives (when the threshold is low) and more seriously, false negatives (when the threshold is high). We introduce the Second Layer in order to tackle this issue.

The Second Layer. The second tier is the Game-theoretic component of the model. We consider the game between the fraudster and the FDS to be a multi-stage repeated game. This is essential because, firstly, the fraudster is likely to try again even if he fails with one card and secondly, no effective learning can take place if the game is considered to be a one-shot one.

It is also worthwhile to mention that the game being played between the FDS and the fraudster is one of incomplete information since the fraudster would be completely unaware of the modus operandi of the Detection System. However, the fraudster is likely to have some notions or beliefs about the strategy of the FDS, as stated earlier. For example, it may be intuitive for him to believe that the FDS may raise an alarm if he carries out a very high-valued transaction or if he attempts a high value transaction of a saleable item like jewelry. Further, since we assume that the situation is one of repeated games, the fraudster can use his past experience to build upon his belief about the FDS strategy. This phenomenon, called 'learning' in game-theoretic terms, will help him to realize and then play according to a Nash Equilibrium (NE) such that he cannot play anything better given the strategy of the FDS. The FDS, as the other player, needs to choose its own best strategy to counter this. One may realize that the advantage of this approach is that this component is not one-time rule-based but will anticipate the next move of the opponent using Game-theoretic strategies. In the realm of Information Warfare, anticipating the next move correctly is a definite advantage to either player. The architecture of the proposed Credit Card Fraud Detection System is depicted in Figure 2.

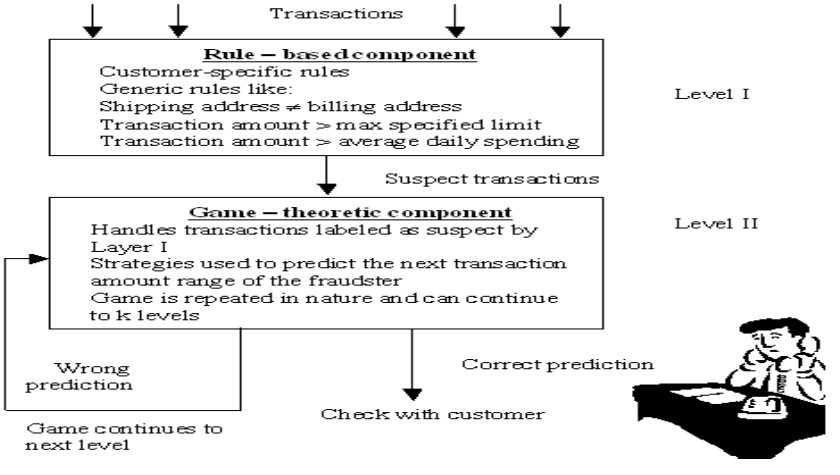


Fig. 2. Architecture of the proposed fraud detection system

The flow of events as would occur in the FDS have been depicted in Figure 3. The transaction for a particular card number is checked at Layer I. If it clears the checks at Level I, it is logged in the master database, failing which it is passed to the Game-theoretic component and the card is marked as suspect. This signifies

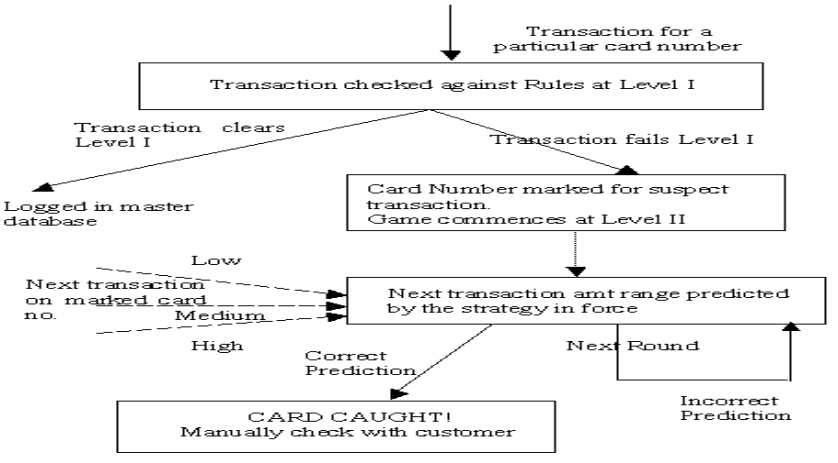


Fig. 3. Flow of events

the beginning of the game between the thief and the FDS. Layer II predicts the next move of the thief and in the event of the prediction being correct, the card is declared as caught.

4 Experimental Results

Our work is primarily focused on the design of a credit card FDS based on a Game-theoretic approach, but unavailability of real credit card data proved to be a serious handicap for testing our system. This was anticipated since real credit card data is treated as confidential by credit card institutions and not released to the public. As one of the solutions to this problem, we invited students from our institute, hereby termed as volunteers, to interact with the system. This was beneficial because firstly, the interaction by the users of the system helped us to capture real data that would be expected in a credit card transaction database. Secondly, it is difficult to model human behavior, whether of genuine cardholder or fraudster, in the absence of real data. The experiment provided us with an opportunity to do so. Lastly, the experiment enabled us to try out the efficacy of our Game-theoretic algorithms.

The three different prediction strategies that were implemented to work in parallel are as follows.

4.1 Tit-for-Tat Strategy

The Tit-for-Tat strategy works well in a wide variety of environments and won the worldwide competition for the well-known "Prisoner's Dilemma", played repeatedly [24]. Since the fraudster is playing a game in which he has no notion of the strategies being used by the opponent, he is likely to be guided by the outcomes of the preceding rounds. For example, if he is successful in carrying

out a particular type/range of transaction, it is likely that he may try a similar transaction again.

4.2 Mixed Strategy

The second strategy implemented in the FDS was a mixed strategy. Though the payoffs are not common knowledge, we propose that the FDS assigns arbitrary payoffs when the game is initiated and predicts the next move according to the mixed strategy derived from these payoffs. This constitutes the initial belief of the FDS and will be strengthened/weakened as the game proceeds in a repeated game scenario. For example, consider that the FDS assigns a very high payoff for the thief to carry out a high value transaction at step k. Therefore, the FDS will predict that the fraudster is likely to undertake a high value transaction with a high probability. Assume that contrary to this, the fraudster opts for a low value transaction instead, at step k + 1, and repeats it at step k + 2. Thus, we can say that, the FDS may need to re-work its belief after x unsuccessful predictions. We assigned the thief's payoffs proportional to the transaction amount and a comparatively large negative payoff for getting caught as shown in Figure 4.

		FDS		
		I	II	III
Thief	I	-80,80	10,-10	10,-10
	II	20,-20	-80,80	20,-20
	III	50,-50	50,-50	-80,80

Fig. 4. Payoff matrix for mixed strategy

4.3 Strategy Based on Markov Models of Game

The Tit-for-Tat strategy is strictly pure since it predicts the last move of the opponent as the next predicted move. We propose that though there is a high probability of a fraudster repeating his last move (as would be predicted correctly by Tit-for-Tat), there is a finite probability for the fraudster to attempt a transaction in a different range, like possibly to increase his payoff. This can be modeled as a Markov chain, in which we model the different transaction amount ranges as distinct states. The last suspicious transaction submitted to Layer II is said to be the present state of the fraudster. A fraudster can be expected to stay in his present state with probability p1 but can also be expected to transit to the other two states each with probability p2, where p1 >> p2, as shown in Figure 5.

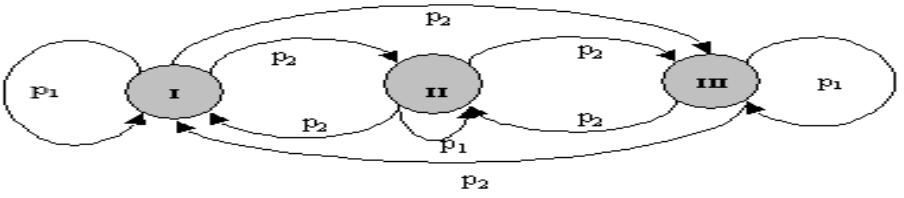


Fig. 5. Strategy based on Markov Models of game

4.4 Results

The volunteers participating in the game were issued with randomly generated credit card details required for an online transaction. Each volunteer was supposed to have 'stolen' these details. The volunteers could carry out online purchases at an intranet site hosted specifically for this purpose. The volunteers were issued with a new card number, if the previous turned invalid, in order to validate that learning can happen in a repeated game scenario.

To evaluate the results, we state that, given the application of credit card fraud detection, a strategy can be said to be efficient if it meets the following criteria.

(a)Predicts the next move of the opponent correctly in the least number of rounds. This ensures that the card is flagged or turned 'invalid', thus, minimizing the losses.

(b)Minimizes the false negatives, that is, accurately predicts the next transaction amount range, for a suspected card number.

The Game-theoretic prediction strategies were tried out in two phases. In the first phase of the study, we classified the online purchases into three ranges. Thus, any submitted transaction could classify either as a low value, a medium value or a high value transaction. The Game-theoretic component would predict the next transaction amount range for a particular card number, if classified as suspect. In the event of the next transaction amount range being the same as the prediction, the transaction was classified as fraudulent and the card number declared invalid. A notion of the opponent's behavior for his move in the second round and a comparison of the three strategies in the first phase of the experiment, with respect to efficacy in predicting that move correctly, have been shown in Figure 6. For this phase, mixed strategy proved to be more efficient in predicting the next move of the opponent. It was also observed that the volunteers were not able to learn the strategies easily especially because the information is imperfect both in terms of strategies and the ranges.

After our initial experiment, we decided to reduce the ranges to two, instead of three, and give the opponent's a better chance of learning the strategy of the FDS. Note that the ranges for the second and third strategy were not changed.

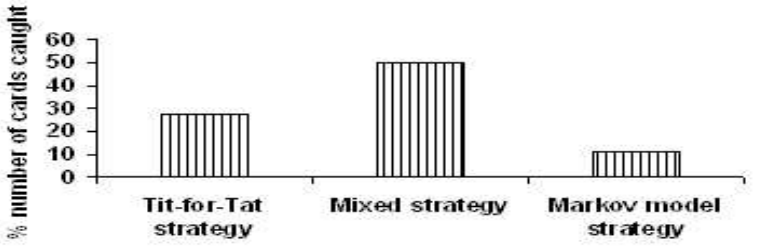


Fig. 6. Second move prediction comparison – first phase

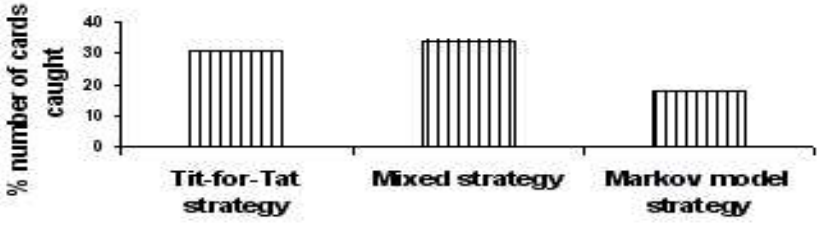


Fig. 7. Second move prediction comparison - second phase

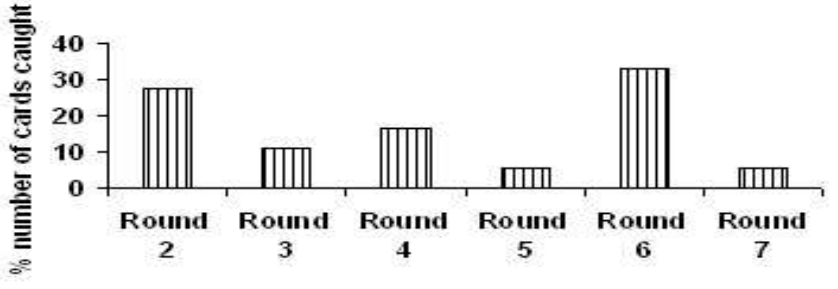


Fig. 8. Performance of Tit-for-Tat strategy - first phase

A comparison of the three strategies, in the second phase of the experiment has been shown in Figure 7.

We used the Tit-for-Tat strategy to return results to the volunteers and to observe their ability to learn the same. Figures 8 and 9 depict the number of cards that were caught in each round in the first phase and the second phase of the experiment, respectively. It was observed that the performance of Tit-for-Tat was better in the initial rounds but the volunteers who learnt the strategy (approximately, if not exactly) were successful in playing longer.

The performance of the three strategies, with respect to failure in predicting a fraudulent transaction correctly, that is, the number of false negatives is shown in Figure 10. It may be noted that since the players were effectively playing

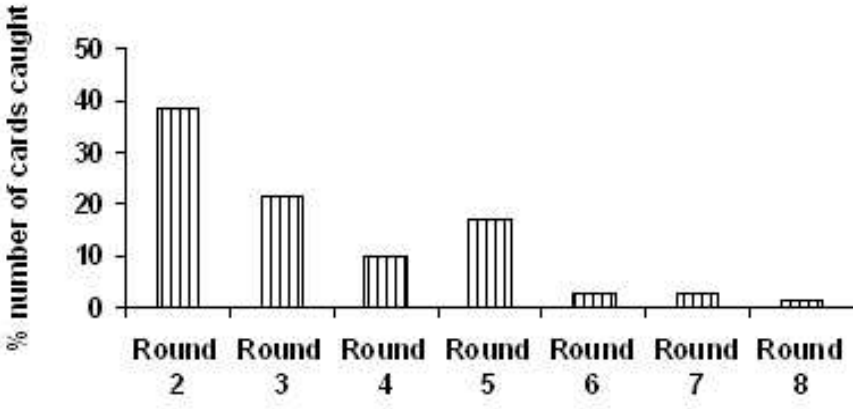


Fig. 9. Performance of Tit-for-Tat strategy - second phase

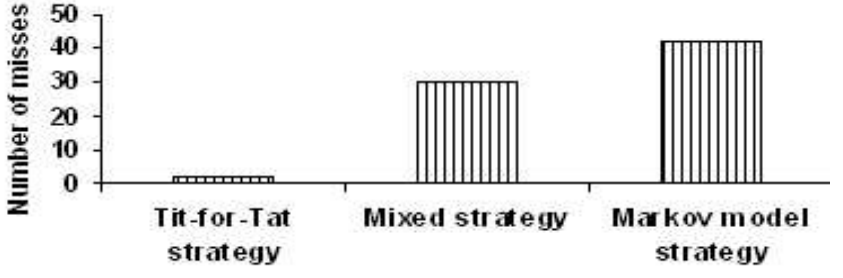
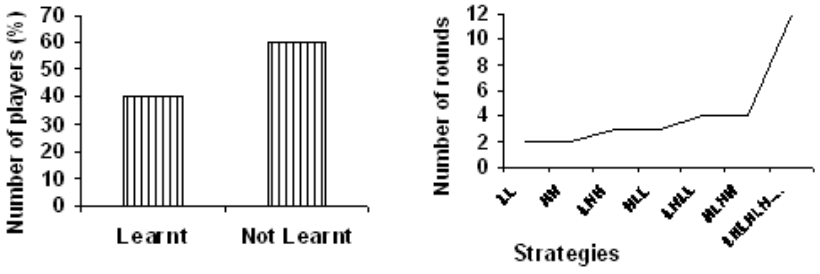


Fig. 10. Comparison of number of misses

with Tit-for-Tat strategy, it was possible that the transaction was predicted to be fraudulent correctly earlier by this strategy as compared to the other two strategies, resulting in a miss by the other two.

The number of volunteers who were able to successfully learn the strategy as a percentage of the total number of volunteers who played is depicted in Figure 11(a). Though a majority of the volunteers were not able to learn the strategy, 40% of them were able to do so. This proved to be an interesting result since it validated the hypothesis that learning does take place in the scenario being considered. For a fixed set of strategies of the FDS, the thief may initially be able to carry out a few transactions but eventually, he will be able to learn his best strategy (or the Nash Equilibrium strategy) against the FDS and can carry out 'n' transactions. The effect of playing with NE strategy, which was LHLHLH or HLHLHL for the second phase of the experiment, vis-a-vis other strategies has been depicted in Figure 11(b). It is pertinent to note that while we demonstrate 'learning' for the fraudster, we intend to build upon the approach by way of learning for the FDS. This would enable the FDS to strengthen its belief about the fraudster and switch to an alternate counter-strategy during the course of play.



(a) (b)

Fig. 11. (a) 'Learnt' vs. 'Not Learnt' (b) Payoff of thief with different strategies

5 Conclusions

The functional approach for most of the intrusion detection systems are rule-based mechanisms, however, they suffer from the limitation that the fraudster may eventually learn the methodology being employed. We have discussed a novel approach of using Game theory in the domain of credit card fraud detection and described the proposed architecture of such a system. We observed that though learning is slower with complex strategies, it does take place in a multi-stage game. We have demonstrated that the approach was validated by the thief being able to learn the strategy of the FDS. Conversely, in a two-player game, between the thief and the FDS, it is indeed also possible for the FDS to learn the strategy of the thief at every step and adopt a counter strategy so as to minimize his payoff. Our approach is not strategy-specific and other heuristic game-theoretic strategies can be included to further improvise the system. Though we have tackled a specific application, we feel that Game theory can be effectively used to counter intrusion in databases in general. We intend to develop a simulator to model the different behaviors of genuine cardholders as well as the fraudster and test the performance of the proposed system on a larger-scale with the simulated data.

Acknowledgements

This work is partially supported by a research grant from the Department of Information Technology, Ministry of Communication and Information Technology, Government of India, under Grant No. 12(34)/04-IRSD dated 07/12/2004.

References

1. T. Chiueh, D. Pilania, *Design, Implementation and Evaluation of a Repairable Database Management System*, Proceedings of ACSAC 2004, 179-188, 2004.

2. C.Y. Chung, M. Gertz, K. Levitt, *DEMIDS: A Misuse Detection System for Database Systems*, Third International IFIP TC-11 WG11.5 Working Conference on Integrity and Internal Control in Information Systems, 159-178, 1999.
3. V.C.S. Lee, J.A. Stankovic, H.S. Son, *Intrusion Detection in Real-Time Database Systems via Time Signatures*, Proc. Sixth IEEE Real Time Technology and Applications Symposium (RTAS 2000), 124-133, 2000.
4. Y. Hu, B. Panda, *Identification of Malicious Transactions in Database Systems*, Seventh Int. Database Engineering and Applications Symposium (IDEAS), China, 329-335, 2003.
5. S.N. Hamilton, W.L. Miller, A. Ott, O.S. Saydjari, *The Role of Game Theory in Information Warfare*, Fourth Information Survivability Workshop, 2002.
6. S.N. Hamilton, W.L. Miller, A. Ott, O.S. Saydjari, *Challenges in Applying Game Theory to the Domain of Information Warfare*, Fourth Information Survivability Workshop, 2002.
7. P. Liu, L. Li, *A Game-Theoretic Approach for Attack Prediction, Technical Report*, PSU-S2-2002-01, Penn State University, 2002.
8. http://www.haveninternet.com/welcome.htm, Complete Website and e-commerce solutions, (20 Apr 05).
9. http://www.aaa-merchant-account.com/, Merchant account credit card processing, (20 Apr 05).
10. http://www.clearlybusiness.com/cb/articles/, Clearly Business âĂŞ Card Fraud, (20 Apr 05).
11. http://sellitontheweb.com/ezine/news0434.shtml, Online fraud is 12 times higher than offline fraud, (20 Apr 05).
12. Y. Li, X. Zhang, *A Security-Enhanced One-Time Payment Scheme for Credit Card*, 14th International Workshop on RIDEâĂŹ04, 40-47, 2004.
13. M.E. Peters, *Emerging eCommerce Credit and Debit Card Protocols*, Proc. 3rd International Symposium on Electronic Commerce, 39-46, 2002.
14. S.H. Low, N.F. Maxemchuk, S. Paul, *Anonymous credit cards and their collusion analysis*, IEEE/ACM Transactions on Networking, 809-816, 1996.
15. S. Ghosh, D.L. Reilly, *Credit card fraud detection with a neural network*, Proc. 27th Annual Hawaii International Conference on System Sciences, 621-630, 1994.
16. E. Aleskerov, B. Freisleben, B. Rao, *CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection*, Proc. Computational Intelligence for Financial Engineering (CIFEr), 220-226, 1997.
17. P.K. Chan, W. Fan, A.L. Prodromidis, *S.J. Stolfo, Distributed Data Mining in Credit Card Fraud Detection*, IEEE Intelligent Systems, 67-74, 1999.
18. M. Syeda, Y.Q. Zhang, Y. Pan, *Parallel Granular Neural Networks for Fast Credit Card Fraud Detection*, Proc. FUZZ-IEEE 2002 Int. Conference, 572-577, 2002.
19. http://plato.stanford.edu/entries/game-theory/, Game Theory, (26 Apr 05).
20. A. Kydd, Formal Theory for Political Science âĂŞ Lecture Notes, 2002.
21. T.S. Ferguson, C. Melolidakis, *On the Inspection Game*, Naval Research Logistics 45, 327-334, 1998.
22. M. Kodialam, T.V. Lakshman, *Detecting network intrusions via sampling: A Game-theoretic Approach*, Proc. IEEE INFOCOM 2003, 1880-1889, 2003.
23. M. Maschler, *A price leadership method for solving the inspectorâĂŹs non-constant sum game*, Naval Research Logistics Quarterly 13, 11-33, (1966).
24. http://www.abc.net.au/science/slab/tittat/story.htm, âĂIJTit for TatâĂİ, (28 Apr 05).