Improvement of Persian Spam Filtering by Game Theory

Seyedeh Tina Sefati
Department of Tabriz Campus
University of Tabriz
Tabriz, Iran

Mohammad-Reza Feizi-Derakhshi
Department of Computer
University of Tabriz
Tabriz, Iran

Seyed Naser Razavi
Department of Computer
University of Tabriz
Tabriz, Iran

***Abstract*—There are different methods for dealing with spams; however, since spammers continuously use tricks to defeat the proposed methods, hence, filters should be constantly updated. In this study, Stackelberg game was used to produce a dynamic filter and the relations between filter and adversary were modelled as a turn game in which there is a leader and a follower. Then, an attempt was made to solve the game as an optimization program via the evolutionary stable strategy (ESS). The dataset used in the study for evaluating and analyzing the proposed method was a real dataset including the emails of four users' personal emails. The results of the conducted evaluations and investigations indicated that the proposed method had an 8% improvement over the three-class classification method and a 0.8% improvement over the ESS-based equilibrium point method.**

Keywords—Spam Filtering; Game theory; Stackelberg game; Evolutionary Stable Strategy; Email Classification; Stackelberg equilibria

I. Introduction

misuse of email is becoming an increasingly serious problem for both individuals and organizations, The occurrence of more and more spam has made up great threat to the security of the internet, it not only occupies numerous network bandwidth and causes great network resources, but also affects people's normal life. Since spammers know some ways not to be recognized, techniques are discussed which may detect and filter spams out of legal emails; indeed, such techniques and methods can be applied on words, phrases or specific fields. Nevertheless, even such good and acceptable filters sometimes fail to accurately classify unsolicited messages. The two chief categories in technique classification are list-based methods and content-based methods. Recently, content-based methods have attracted more attention and interest; The reason for the less popularity of list-based methods in comparison to content-based ones is that list-based methods have fixed rules and regulations which need to be updated frequently. Spammers usually make some changes on spams so that filter would identify them as regular and normal mails.

In this study, the behavior and relation between adversary (spammer) and spam filter (classifier) was investigated. In the method introduced in the present study, relation between spammer and filter modelled as a sequential Stackelberg game and filters detect spams by learning the adversary's behavior. On the other hand, adversary try to deceive filters by learning their parameters. For finding the equilibrium point of the game in infinite case, evolutionary stable strategy (ESS) was used here.

The entire paper is divided into five sections. Section II provides the related works. In III we formulate Stackelberg games with infinite strategy space for spam detection and Then, explain the evolutionary stable strategy to find the needed equilibrium. in section IV we describe the experimental setup and presents and discuss the experimental results. And it followed by conclusion in section V.

II. Related Works

Numerous methods have been proposed in the literature for dealing with unsolicited emails and researchers continue introducing new methods for managing the different extensive dimensions of spams. As a case in point, list-based methods such as black list, white list and grey list can be mentioned. By classifying senders into the two category of spam and legal senders, these filters try to identify spams. Although these filters are simple, they are not adequately efficient because they possess fixed rules and regulations which can be identified and eluded by spammers. In [1], methods were discussed in which they change addresses to detect spams as emails and also to detect websites which spammers use to hide their webpages. In [2], DNSBL was used for analyzing the behavior and the efficiency of the black list and the elimination power and the conditions at which black list is not used have been discussed. The results showed that combining black listing with a spam refining program can have higher efficiency.

Due to the shortcomings of the list-based methods, content-based methods which are categorized into word-based, rule-based and statistical filtering methods gained more popularity and attraction. Machine-learning methods are a kind of content-based methods. Each of the machine learning methods can have acceptable performance, the studies [3], [4], [5], [6], [7] demonstrated the positive effect of pre-processing and feature selection in machine learning methods such as Naïve Bayesian, Support Vector Machine, K-Nearest Neighbor, Artificial Neural Network and Decision Tree. Also, the combination of these methods leads to the improvement of the precision [8]. Based on the results of the studies reported in [9], [3], [8], [10], [11] and [12], it can be maintained that NB is one of the strongest available algorithms for categorizing emails which uses probabilities for detecting the class of new data.

Also, filters, it is deceived less than list-based filters. In general, each of the machine-based learning methods has its own merits and demerits. According to the findings reported in [4] and [5], the benefit of SVM method is that it can solve the problem of finite samples. However, it should be noted that the Kernel function and c parameter should be determined correctly for it. A function was proposed for kernel in [13]. The main challenge of the artificial neural networks is determining the number of nodes in the secret layer and the number of appropriate repetitions for finding weight. Nevertheless, despite having high precision, extensive calculations are one deficiency of the artificial neural network [6], [7], [14], [15] .The simplicity of implementation and the ease and speed of learning with regard to KNN have resulted in the popularity of KNN. At the same time, it should be noticed that the specification of similarity criterion and the selection of the appropriate number of neighbors (k) are the main problems of this algorithm [16]. Decision tree is a common method in data-mining which is easy to understand and evaluate. The exponential growth of the decision tree in line with problem growth is a challenge of this algorithm. Hence, NBTree and J48 were proposed to sort out this issue [17].

Inasmuch as spammers try to deceive filters by changing the content or components of emails, hence, investigating the behavior of the spammer and considering his actions will lead to the optimization of the email classifying methods. The issue of learning adversary's behavior was first proposed in [18] where a game between spam filter and adversary was proposed. However, since any changes in the players will make this method non-executable, hence, it is practically unusable. For solving this problem in [19] and [20], spam senders try to identify filter parameters by first learning the adversary's behavior and reverse engineering; next, they plan their attacks based on it. In this method, there is no equilibrium point for the adversary and spam filter [21]. Also, in [22], adversary's learning model was designed based on game theory. The rationale behind this modelling is to achieve an equilibrium point for the adversary and spam filter and it is assumed that filter and adversary have full understandings of each other's behavior. The genetic heuristic algorithm was used for solving this game in the unlimited space and achieving an equilibrium point. In [21], the relations between the adversary and filter was modelled as a turn game where there is a leader and a follower. Then, an attempt was made to solve the optimization program through evolutionary strategies. The results indicated that filtering accuracy rate has been improved in this method. In [23], the relations between spammers and user was modelled as a competitive game. Then, the strategy between them is consequently predicted. Next, the prediction is used for adjusting spam filters. In this method, it was assumed that there is a filter on the system and the user can choose whether he wants to read the received email or the spam. This game has a Nash equilibrium and the objective is to achieve an equilibrium so that the adversary's strategies can be guessed by means of this equilibrium.

III. THE PROPOSED METHOD

The method introduced in this paper is based on game theory which was used to guess the adversary's action and, consequently, adopt the best strategy for the filter. As illustrated in figure 1 for the proposed method, after pre-processing and using a learning algorithm for filtering spams, the relations between adversary and filter was assumed to be of the Stackelberg game type. That is to say, the first player, namely the adversary plays the role of leader and it can impose its own strategy on the second player, i.e. filter. Hence, assuming that the follower selects the best possible decision based the leader's strategy, hence, the leader tries to adopt the most appropriate decision. Then, based on the leader's strategy, the follower reacts with respect to the payoff. In most cases, backward induction is used for finding Stackelberg equilibrium point. In the assumption of the problem, the strategy space for the two players was considered to be complex and unlimited.

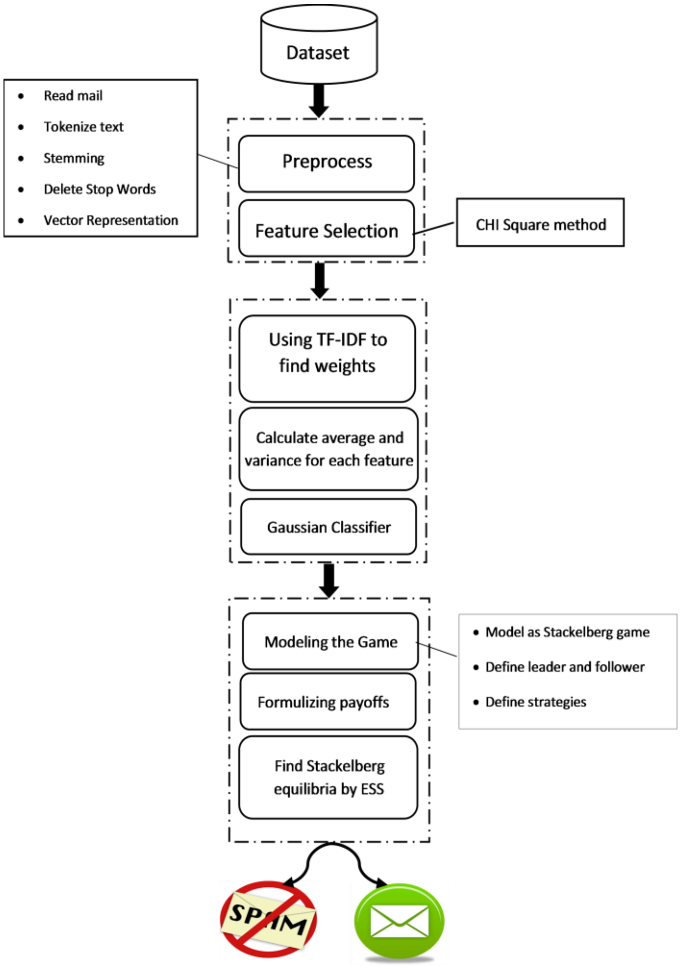

Fig. 1. Schematic View of Proposed Method

A. DataSet

Inasmuch as there was no available Farsi dataset for filtering spam, the dataset used in the study included personal emails of 4 users for approximately 8 months which were collected in 2012-2013. The dataset which was collected by the researchers included 682 legal emails and 629 spams. Tagging was used for isolating email sections. Among the collected emails from the dataset, about 80% was used for learning system and 20% was used for the testing phase.

B. Preprocessing

Email classification methods are similar to text classification methods. Figure 2 depicts the text classification. For doing the preprocessing stage for each user, at first, spam classes and legal classes should be read from the related folder and the class of each one should be specified. After reading the content of emails from each class, the available words in the email which were obtained from the body and title parts were separated token by token and the emphasis words and the stop words were eliminated. Next, the words were extracted from inside of the emails; then, the obtained words were illustrated in a vector based on their frequencies. Next, using CHI method [24] and [25], some words which could distinguish classes from one another were selected as the best words. Afterwards, by weighing words via TF-IDF method [26], the weight related to each feature was calculated; then, feature mean and variance were calculated for class which were used in the next stage.

C. Game modelling

It was assumed that data belong to a specific one-dimensional space and they are distributed normally. Spam distribution is determined by $S \sim N(\mu_s, \sigma_s)$ and legal email distribution is determined by $H \sim N(\mu_H, \sigma_H)$. İn the game, spammer plays by moving the boundary towards μ_H and also filter tries to maximize its payoff by changing the boundaryline.

The initial state of the game is illustrated in figure 3. TPs stand for spams which are truely spams but FPs are legal emails which were wrongly classified as spams. Moreover, TNs are the legal emails which are correctly classified but FNs denote wrongly classified spams. Adversary's purpose is to enhance the number of FNs. Hence, it will lead it message feature space towards the space of legal email feature (figure 4). In contrast, as the filter notices the adversary's strategy and system learning for a second time, it determines the best threshold (figure 5).

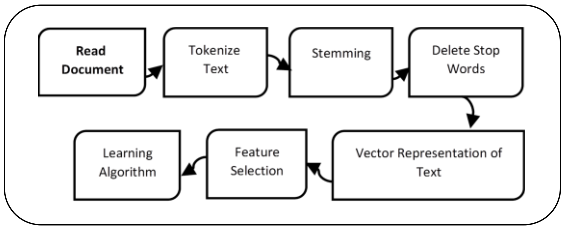

Fig. 2. Text Preprocessing

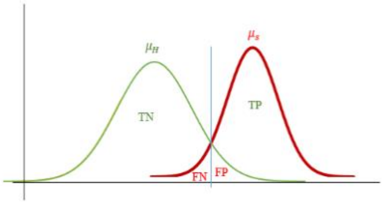

Fig. 3. Initial state of the game between spammer and filter

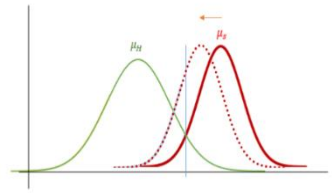

Fig. 4. adversary's strategy

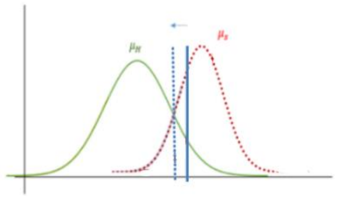

Fig. 5. filter's strategy

The ultimate goal of the game is to achive the equilibrium point. Assuming that players are aware of one another's payoff function, the purpose function of the players will be used to examine it. Then, ESS is used to calculate the equilibrium point of the game.

D. Stackelberg equilibrium point

Each player consists of a set of strategies which are labelled as U and V for the leader and the follower, respectively; also, u and v denote the feature space of them, respectively. Furthermore,each player has one differentiable payoff function which is defined as $J_i(\mathrm{U},\mathrm{V}) \rightarrow \mathrm{R}$. U and V are bounded and convex and regarding the adversary player's movement, the strategy is defined in the following way [22]:

$$R_L = \arg\max_{v} J_{\,L}\,(u,v)$$
$$R_F = \arg\max_{u} J_{\,F}\,(u,v) \quad (1)$$

Stackelberg equilibrium point is an equilibrium in which until the time the player sticks with its own selected strategy, none of the other two players have any motivations for changing their strategies [21].J^i Refers to the cost function for i player. The best response for each i player is denoted by $\mathrm{R_i}$. One solution for the Stackelberg equilibrium is produced by the following method [21]:

$$\mathbf{u}^* = \mathbf{arg}\ \max_{\mathbf{u}\epsilon\mathbf{U}}\ \mathbf{J^L}(\mathbf{u}, \mathbf{R_F}(\mathbf{u})) \quad (2)$$

By doing so, the follower responds whether the optimal value is:

$$\boldsymbol{v}^* = \boldsymbol{R_f}(\boldsymbol{u}^*) \quad (3)$$

One mathematical method for obtaining Stackelberg equilibrium in two-player games is to apply bi-level programming problem [27]. In this study, equation 8 can be used as the bi-level programming problem where each player tries to maximize its own payoff [22].

$$\max_{\mathbf{u}}\quad \mathbf{J^L}(\mathbf{u}, \mathbf{v}) \quad (4)$$
$$\mathbf{s.t\ g}(\mathbf{u}, \mathbf{v}) \leq \mathbf{0}$$
$$\mathrm{v} \in \arg\ \max_{\mathrm{v}}\ \{\ \mathrm{J^F}(\mathrm{u},\mathrm{v}) \mid \mathrm{h}(\mathrm{u},\mathrm{v}) \leq 0\ \} \quad (5)$$

In equation 9, h and g variables are the limitations in U and V action spaces. Since bi-level programming problem is regarded as an NP-Hard problem, ESS was used for finding the equilibrium point.

E. *Formulizing payoffs*

Using probability density function in the normal space $N(x,\mu,\sigma)=\frac{1}{\sqrt{2\pi\sigma}}e^{-\frac{(x-\mu)^2}{2\sigma^2}}$, we can obtain cumulative density function$F(t,\mu,\sigma)=\int_{-\infty}^{z}N(t,\mu,\sigma)dx$. The adversary's payoff can be defined as the degree of spams which can pass through filter as legal email-the cost of transmission from one normal space to another normal space (equation 6). In case there is a dataset with several features, assuming that the features are independent, equation (7) is obtained [21].

$$\begin{aligned}\boldsymbol{J_L(u,w)} &= FNR - \boldsymbol{\alpha KLD(\mu_s,\sigma_s,\mu_s-u,\sigma_s)} \\ &= \boldsymbol{F(\omega,\mu_s+u,\sigma_s)-\alpha KLD(\mu_s,\sigma_s,\mu_s+u,\sigma_s)}\end{aligned} \tag{6}$$

$$J_L(U,W)=\frac{1}{q}\sum_{i=1}^{q}J^L(u_i,w_i) \tag{7}$$

q denotes the number of features and KLD is a notion for estimating the impact of transmitting the space of spam the size u on the initial data; indeed, it is a criterion for evaluating the degree of closeness of probabilistic models to the accurate distribution of the population. For measuring the impacts of transmission from $N(\mu_1,\sigma_1)$to $N(\mu_2,\sigma_2)$, equation (8) is used [22].

$$\begin{aligned}&\boldsymbol{D_{KL}(N_1,N_2)} \\ &= \boldsymbol{\frac{1}{2}\left(log\left(\frac{det\Sigma_2}{det\Sigma_1}\right)\right)+tr\left(\Sigma_2^{-1}\Sigma_1\right)} \\ &+ \boldsymbol{(\mu_2-\mu_1)^T\,\Sigma_2^{-1}\,(\mu_2-\mu_1)}\end{aligned} \tag{8}$$

Filter rewared is interpreted as the enhancement in the rate of correct acceptance and correct rejeaction [22].

$$\begin{aligned}\boldsymbol{J_F(u,w)} &= TPR+TNR - \boldsymbol{\beta(\omega-\frac{\mu_s\times\sigma_H+\mu_H\times\sigma_s}{\sigma_H+\sigma_s})^2} \\ &= \boldsymbol{2F(\omega,\mu_H,\sigma_H)-2F(\omega,\mu_s-u,\sigma_s)} \\ &\quad \boldsymbol{-\beta(\omega-\frac{\mu_s\times\sigma_H+\mu_H\times\sigma_s}{\sigma_H+\sigma_s})^2}\end{aligned} \tag{9}$$

$$J_F(U,W)=\frac{1}{q}\sum_{i=1}^{q}J^F(u_i,w_i) \tag{10}$$

α

adjusts the distance criterion on the degree of spam space transmission. İts enhancement leads to FNR reduction. In contrast, by controlling the degree of movement of w, β leads to the FPR reduction. İn case zero is selected for both parameters, $\frac{\mu_s+\mu_H}{2}$ will be considered as the threshold algorithm. Moreover, since both parameters are zero, the adversary will not pay any cost for transmission. As a result, by selecting the highest transmission value, spam space will be completely consistent with the space of legal emails. Under this condition, the degree of system error will be 50%; in fact, α can not practically be zero. As more value is regarded for α, the adversary will have to pay more cost. Consequently, a smaller value is selected for u. in case β has the value of zero, the system will not distinguish between wrong and right pass rate. However, as β increases, filter will hardly change the threshold. Consequently, a value close to the previous threshold value will be selected. This parameter can be used to distinguish between wrong and right pass rate. In other words, it can be used for weighing.

F. *Evolutionary stable strategy (ESS)*

In case ESS strategy is selected by all the members of a population, no other mutation strategy can overcome it. If a strategy is evolutionary and stable, hence, there will be Nash equilibrium but the requirement for the evolutionary stability of a Nash equilibrium is that it will be a strict Nash equilibrium.

TABLE I. TECHNICAL SPECIFICATIONS OF EVOLUTIONARY STABLE STRATEGY

Initial population	$u\epsilon[\mu_H,\mu_s]$ and $w\epsilon[w,\mu_H]$ K random conversion of u and w
Parents' selection	random
Fitness function	Each player maximizes his or her payoff
mutation	Gaussian mutation with zero average and l standard deviation
Termination condition	Particular number of generations

In most studies and books, ESS method has been considered for the symmetrical games. Nevertheless, in this study, there are two non-symmetrical (different) players. Player I has the strategies of i=1,2,…, m and player J has the strategies of j=1,2,……..,n. at any moment, p_i and q_j indicate the selection of i and j by the players I and J, respectively. p = $(p_1,\dots,p_m)$ and q = $(q_1,\dots,q_n)$ are the probabilistic vectors which determine population status together. The fitness of i is denoted by F(i) and the fitness of j is denoted by G(j) which depend on (p,q) at the given moment. Hence, the fitness function is defined as F(i|p,q) and G(j|p,q).

Overall schematic view of the proposed algorithm: ESS(evolutionary stable strategy)

1. Initial population is randomly created
2. Players play together and the profitability of each strategy is measured.
3. The strategies with more profitability values are reproduced in society.
4. Steps two and three are repeated until the society achieves stability.
5. Some members begin to change their own strategies (mutate).
6. Until reaching the termination condition, algorithm is repeated from step 2.

Fig. 6. schematic view of the proposed algorithm

IV. EXPERIMENS & RESULTS

In the experimental phase, after training the system by the training data (80% of samples), test data (20% of samples) is used for evaluating system. The results of experiments are given below in the form of tables and figures.

Evaluation criteria: in text classification problems, the following criteria are usually used:

$$accuracy=\frac{TP+TN}{TP+TN+FP+FN} \tag{11}$$

$$precision=\frac{TP}{TP+FP} \tag{12}$$

$$recall=\frac{TP}{TP+FN} \tag{13}$$

$$F_1 = \frac{2*(precision*recall)}{precision+recall} \tag{14}$$

A. Results of training phase

As mentioned before, game model was produced in the training phase and was executed on each component of dataset; then, using ESS which was proposed in [21] and the ESS of the equilibrium point, the results were measured. The higher the adversary payoff and the higher the filter payoff, the algorithm will be more precise and accurate. Variables of the problem were evolved in 100 generations and the best member of each generation was used. Similar to the study reported in [21], the value of α parameter in the Kullback-Leibler equation was considered to be 0.01. As illustrated in figures 7 and 8, it can be argued that ESS method is far better than ES (evolutionary Strategy).

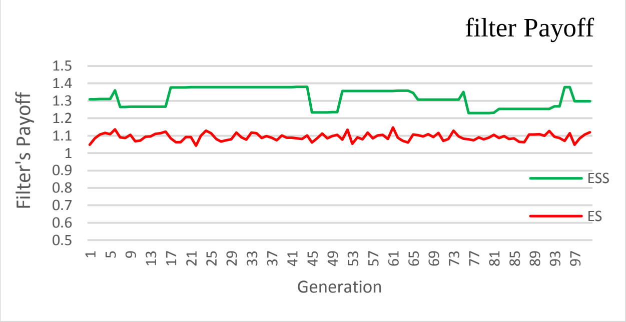

Fig. 7. average filter payoff with one feature on Evolutionary Strategy and Evolutionary Stable Strategy

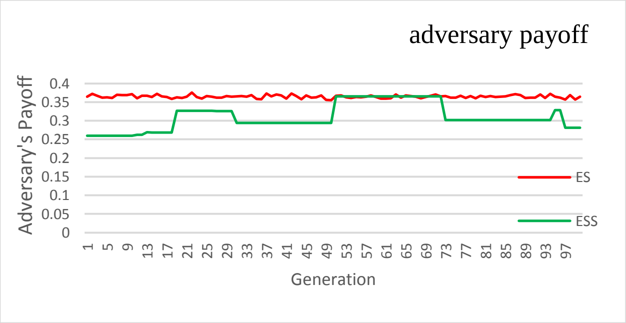

Fig. 8. Average adversary payoff with one feature on Evolutionary Strategy and Evolutionary Stable Strategy during 100 generations

For a second time, algorithms were executed separately for 100 features and average payoffs were taken into consideration. 90 samples were used for training. Payoff function is linear and the problem variables were evolved in 100 generations.in each generation, average chromosomes were given (not the best chromosomes). The payoff which is obtained for ESS is the best chromosome of the generation because, at the end of each execution, strategies are stabilized and all of them become identical. Regarding these issues, as depicted in figures 9 and 10, it can be maintained that, in most cases, ESS has better performance than ES. Furthermore, with respect to the results, it can be observed that 100 generations are not sufficient for evolution. Hence, more repetitions are need for achieving evolution. However, since there is not one equilibrium point, it can be argued that, in 100 generations, a near-optimal response can be achieved. Based on the strategy of the opposite side, payoffs in each generation can be more or less because each player not only has unlimited strategy space and acts smartly but also it is aware of the strategy of the other side. Based on the other side's strategy, it selects the most appropriate condition for itself.

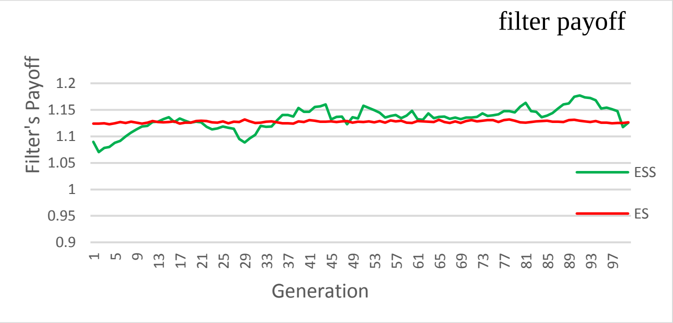

Fig. 9. Average filter profits for 100 features on Evolutionary Strategy and Evolutionary Stable Strategy in 100 generations (average chromosomes)

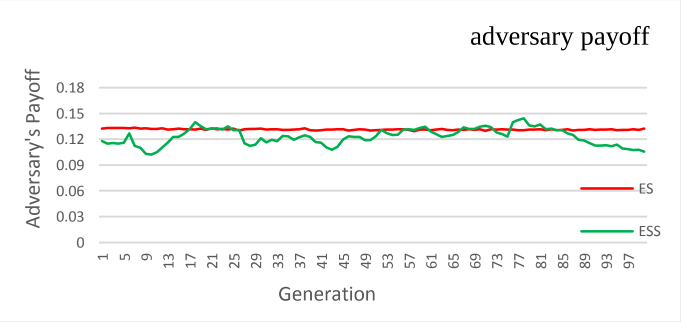

Fig. 10. average adversary's profits for 100 features on Evolutionary Strategy and Evolutionary Stable Strategy in 100 generations (average chromosomes)

B. Results of the experimental phase

In this phase, the final position of the filter and adversary at the equilibrium point were obtained for each feature by the data of the training phase. Then, these positions were used to obtain the following evaluation criteria:

- One sample is selected from each dataset of the experiment phase. It should be specified that each feature dedicates the sample to which classification.
- Class label for all the features of the sample is determined by the previous method.
- The sample class depends on the largest number of labels which is specified by the features.

The researcher and collector of the dataset has argued that 65 samples and 90 features are the best and most desirable number of samples and features for training and testing in his own research; she used the same number of samples and features in his evaluations. In a similar vein, in this study, 90 features and 65 samples were used to test the implementation methods. The average evaluation criteria were used and the equilibrium point was measured by the ES and ESS which are given in table 3.

The highest precision was desirable in the system used in this study because the higher is the precision, the lower will be the wrongly accepted rate. Indeed, it should be noted this issue is of high significance in filtering and investigating spams. The obtained results indicated that the precision of the filter for the modelling method and solving the game by ESS and ES was better than those of other methods.

TABLE II. AVERAGE EVALUATION CRITERIA FOR FINDING GAME EQUILIBRIUM POINT BY ES AND ESS ON REAL DATASET

	Before	ES	ESS
Accuracy	0.764877	0.795356	0.796081
Precision	0.887694	**0.894732**	**0.902213**
Recall	0.628447	0.693759	0.703919
F1	0.712426	0.754676	0.755538

TABLE III. RESULTS OF THREE-CLASS CLASSIFICATION FOR FARSI EMAILS BASED ON THE CRITERIA: PRECISION, RECALL AND F ON REAL DATASET

	NB	SVM	KNN
Precision	86/225	**86/425**	83/875
Recall	85/15	**85/175**	84/65
F1	**85/775**	85/075	85/6064

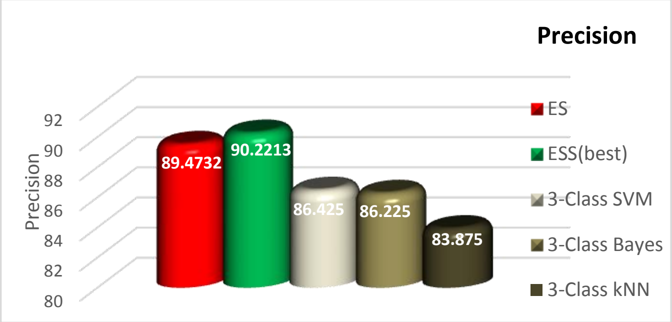

Fig. 11. Comparison of average accuracy of the results of the proposed method with those given in [9]

As showed in Figure 11 the methods of Stackelberg game and finding the equilibrium point by ES and ESS had 89.4% and 90.22% which achieved the highest precision among other methods. It should be noted that the method used in [9] which had used three-class classification on the dataset of Farsi emails had the precision value of 86.42%.

V. CONCLUSION AND DIRECTION FOR FURTHER RESEARCH

In the present study, game theory was used to investigate the relations between filter and adversary and the detection of spams by filter was considered. Regarding their payoff functions, the two players selected the best strategies. After repeating the game, they reached an equilibrium point. It should be pointed out that both players played smartly and they were interested in enhancing their own payoffs and, consequently, favored a reduction in the adversary player's payoff. The results of the experiments indicated that the evolutionary stable strategy (ESS) was able to find game equilibrium point with more precision than ES method. That is, ESS had 79.6% accuracy rate, 90.2% precision, 75.5% F criterion and 70.3% recall. In contrast, ES had 79.5% accuracy rate, 89.4% precision, 75.4% F criterion and 69.3% recall. Since speed and time are of high significance in modern life, as a direction for further research, we should focus on reducing and optimizing training time in future studies.

REFERENCES

[1] K. Bhargrava, D. Brewer and K. Li, "A Study of URL Redirection Indicating Spam," in Sixth Conferance on Email and Anti-Spam, Mountain view, California, 2009.

[2] S. Tomas and F. Radim, "Improving efficiency of e-mail communication via SPAM elimination using blacklisting," in 21st Telecommunications forum TELFOR, 2013.

[3] T. A., M. E. and K. N., "An Evaluation of Machine Learning Techniques for Enterprise Spam Filters," 2004.

[4] R. Shams and R. E. Mercer, "Classifying Spam Emails using text and readability features Data Mining (ICDM)," in IEEE 13th International Conference, 2013.

[5] W. L. a. L.-F. K. Yuxin Meng, "Enhancing Email Classification Using Data Reduction and Disagreement-based Semi-Supervised Learning," in Communication and Information Systems Security Symposium, IEEE ICC, 2014.

[6] T. Tich Phuoc, T. Pohsiang and J. Tony, "An Adjustable Combination of Linear Regression and Modified Probabilistic," in 19th International Conference on Pattern Recognition (ICPR), 2008.

[7] S. A. Seyyed Hossein and M. Saeed, "Genetic-based Feature Selection for Spam Detection, Electrical Engineering (ICEE)," in 21st Iranian Conference, 2013.

[8] M. T. Banday, "Effectiveness and Limitations of Statistical Spam Filters," in International Conference on New Trends in Statistics and Optimization, Organized by Department of Statistics, University of Kashmir, Srinagar, India, October 2008.

[9] N. Vasfi-sisi and M.-R. Feizi-Derakhshi, "Three-Class Classification of Persian Emails by Naïve Bayes Algorithm," in International Conference on Machine Learning, Electrical and Mechanical Engineering (ICMLEME'2014), Dubai, 2014.

[10] H. Wang, G. Zheng and Y. He, "The Improved Bayesian Algorithm to Spam Filtering," in Proceedings of the 4th International Conference on Computer Engineering and Networks, 2015.

[11] G. Kaur and E. N. Oberai, "Naïve Bayes Classifier with Modified Smoothing Techniques for Better Spam Classification," International Journal of Computer Science and Mobile Computing, vol. 3, no. 10, pp. 869-878, October-2014.

[12] Y. Zhang, X. Yang and Y. Liu, "Improvement and Optimization of Spam Text Filtering System," in 3nd International Conference on Computer Science and Network Technology, 2012.

[13] Y. L., Z. Z. and J. Z., "A word sequence kernels used in spam filtering," Academic Journals, vol. 6, pp. 1275-1280, 2011.

[14] P. Kumar, P.Kumareasan and S. Babu, "Accuracy Analysis of Neural Networks in removal of unsolicited e-mail," International Journal of Computer Applications, vol. 16, no. 3, Februrary 2011.

[15] S. Shaveen, C. Anish and P. L. Sunil, "Improving Spam Detection Using Neural Networks Trained by Memetic Algorithm," in Fifth International Conference on Computational Intelligence, Modelling and Simulation, 2013.

[16] P. I. Nakov and P. M. Dobrikov, "Non-Parametric Spam Filtering based on kNN and LSA," in 33th National Spring Conferance, 2004.

[17] S. Chakraborty and B. Mondal, "Spam Mail Filtering Technique using Different Decision Tree," International Journal of Computer Applications, vol. 47, no. 16, 2012.

[18] N. Dalvi, P. Domingos, Mausam, S. Sanghai and D. Verma, "Adversarial classification," in KDD '04 Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining, New York, 2004.

[19] D. Lowd and C. Meek, "Good word attacks on statistical spam filters," in Proceedings of the second conference on email and anti-spam (CEAS), Redmond, WA, 2005/7.

[20] D. Lowd and C. Meek, "Adversarial Learning," in Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining, New York, 2005.

[21] N. Sadigh, S. Hashemi and A. Hamzeh, "SPAM DETECTION BY STACKELBERG GAME," Advanced Computing: An International Journal (ACIJ), vol. 2, no. 2, 2011.

[22] W. Liu and S. Chawla, "A Game Theoretical Model for Adversarial Learning," in Data Mining Workshops, 2009. ICDMW '09. IEEE International Conference, Miami, 2009.

[23] Androutsopoulos, E. F. Magirou and D. K. Vassilakis, "A Game Theoretic Model of Spam E-Mailing," in 2nd Conference on Email and Anti-Spam, Athens, Greece, 2005.

[24] Y. Yang and J. Pedersen, "A comparative study on feature selection in text categorization," 1997 .

[25] M. Bitarafan and S. Jalili, "\increment text classification performance based improve feature selection methods," Journal of the Technical University, vol. 40, no. 3, pp. 313-328, 2006.

[26] Q. Ren, "Feature-Fusion Framework for Spam Filtering Based on SVM," in In Proceedings of the 7th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference, Washington, US, 2010.

[27] L. N. Vicente and P. H. Calamai, "Bilevel and multilevel programming: A bibliography review," Journal of Global Optimization , vol. 5, no. 3, pp. 291-306 , 1994.