Using AOP neural networks to infer user behaviours and interests

Andrea Fornaia, Christian Napoli, Giuseppe Pappalardo, and Emiliano Tramontana
Department of Mathematics and Informatics
University of Catania
Viale A. Doria 6, 95125 Catania, Italy
{fornaia, napoli, pappalardo, tramontana}@dmi.unict.it

***Abstract*—Generally, users of an 'ego' social network provide personal information and actively participate in groups to discuss some topic. We propose a multi-agent driven system to analyse user behaviour and interests by gathering data related to different activities and show that a more comprehensive identity can be built from sparse data, while possibly reveal the tentative of some users to deceive other people. In our approach, user profiles are given to a profiling agent that retains relevant data by using ANN technologies that find categories for users. Even new users, whose profile is still mostly undefined, are given a 'most-likely' category, therefore the traits of such a category are inferred for new users. Since a group in a social network such as Facebook can be seen as a category, the agent driven system is also able to classify user profiles and recommend new groups users can subscribe to, according to their interests and preferences.**

***Index Terms*—Neural Networks, Social Networks, Artificial Intelligence, Security, Multi-agent Systems.**

I. Introduction

Trust and reliability of data available on social networks are important concerns for both service providers and subscribers. Given the large size of a social network, in terms of subscribers, data exchanged, and number of links (such as friendship, following, membership to groups, endorsements, etc.), it is desirable to have an automatic way to efficiently process data to ensure security and validate at least some contents. User *feature* and *behavioural* analysis are two interesting and important means upon which a solution can be build.

The first step in this direction is to group users into *categories*. Interesting performances have been achieved by systems analysing user interests, however, in general, such systems are only intended for a small context, or for analysing selected users. Even though statistical methods make it possible to characterise features and interests for a single user [1], it is difficult to build a proper analytical model for user interactions due to the vastness of data available in a social network, i.e. number of links, undetermined number of subscriber features, etc. A huge amount of features characterise subscribers, however a relevant portion of values for such features is missing for many subscribers in a real environment, hence a complete formulation of a comprehensive analytical model would be unfeasible [2], [3], [4]. Moreover, the large amount of data and the frequency of changes make the numerous reiterations needed to formulate the analytical model very computationally costly.

Still it is highly desirable to have an automatic analysis that can dynamically incorporate data available on the social network over time. This is fundamental for building advanced services such as e.g. the timely identification of autogenous threats. An automated mechanism should take advantage of soft computing approach such as soft artificial intelligence [5], particle swarm optimisation and positioning [6], [7], [8], evolutionary methods [9], swarm intelligence [10], neural networks [11], etc.... Neural networks has been proven effective for a large number of problems which cannot be solved in terms of a priori mathematical models [12], [13], especially when used with hybrid architectures [14]. We propose an agent driven artificial intelligence system based upon a Radial Basis Probabilistic Neural Network (RBPNN), which is well known for its capability to classify and generalise datasets and can be continuously trained to recognise novel features, hence can easily cope with changing data. The proposed neural network has been embedded into a *Classification Agent* that builds a model out of data coming from user profiles, and handled by other agents, such as a *Profiling Agent* and a *Crawler Agent*, which retain useful data from different parts of an 'ego' social network [15], such as Facebook(R). When analysing a social network, as Facebook, the main difficulties are due to: the unknown number of subscribers, friendship relations, groups, followers, etc.; and the unknown size of data and features for each subscriber. We overcome such difficulties thanks to several agents, which handle data and retain a representation (in our previous analyser version, a big amount of data has been properly processed using a GPU based solution [16], [17], [18], [19]). Specifically, our *Classification Agent*, according to the proposed RBPNN solution, can handle partial data, acting as a modeller for dynamically changing user' s profiles. With our classification approach, we are able to perform early identification of autogenous threats: firstly, an incoherent user profile could be identified when the RBPNN *prediction* of user behaviour, obtained by assigning the user to a category, differs from the actual behaviour; secondly, deception can be revealed by matching user features with others of undesirable categories of users. Moreover, the agent system can use the same classification approach to recommend new groups that fit user interests: this is achieved using group subscriptions as categories, instead of the ones specifically designed by the administrator to classify user behaviour.

Our solution comprises different collaborating agents that make the social network administrators able to classify and monitor the user behaviour for security enforcement, other than enhancing their experience suggesting new groups they can subscribe to, according to their interests.

The rest of this paper is structured as follows. Section II gives the background on the dynamics of a social network. Section III reports about analytical models for classification. Section IV describes the proposed multi-agent system based on RBPNNs. Section V describes the Classification Agent. Section VI and Section VII reports respectively the performed experiments and results. Finally, Section VIII draws our conclusions.

II. Social network dynamics

This work analyses *'ego'* networks and Facebook is considered as a significant representing example. In 'ego' social networks, the *small-world* properties are an important characteristic for the actual social dynamic of the network [20]. Moreover, social networks follow a *scale-free* behaviour [21], i.e. a few nodes (i.e. users) act as important hubs centralising a large number of links, hence data passing through such hubs are widely spread on the network.

A. Clusters of users in a social network

For social networks, such as Facebook, we identify two different kinds of relationships among users. A bidirectional interaction between a pair of users occurs when such a pair exchanges a *friendship*. Additionally, Facebook provides *groups*, i.e. a user is given means to broadcast contents to all the members of the same group where s/he belongs to. We define the mutual exchange of *friendship* between a pair of users as a *strong* connection between the pair, whereas for a pair of users that are *members* of the same group, the membership provides a *weak* connection between such a pair. When a user posts a content into a group, then the resulting one-to-all interaction provides a *weak*, and sometimes *random*, connection with members of the group, who generally share a limited number of interests.

We define the *distance* between a pair of users as follows. When a pair has exchanged a friendship, then the distance is simply 1, otherwise the distance is the minimum count of hops between the pair by following friendship or group connections. Hence, weak connections (available to users belonging to the same group) provide means for information to rapidly flow across users belonging to portions of the social network that have no direct friendship relationship. I.e., weak connections act as *bridges* between users having no friendship, by allowing their *distance* to become equal to 1.

From the friend list of each subscriber we identify *clusters* of users. Clusters consist of users having a higher number of friendships toward users within the same cluster rather than toward users not belonging to the cluster. Analogous to distance between users, we define distance between a pair of clusters as the minimum count of hops between one user on the first cluster from one in the second cluster. Distant clusters can be considered independent parts of the social network that still satisfy the scale-free properties. Clusters generally consist of users sharing a set of interests and activities, and users of the same cluster form a sort of social neighbourhood [22].

Let us suppose that two users belong to different clusters, while being on the same group. When considering the relationship of users and groups, we can see that a group acts as a bridge for the contents to flow from a cluster to another (the clusters of the correspondent users). Hence, different parts of the network become mutually capable of exchanging contents, fostering the small-world behaviour of the social network [23]. In this way, clusters of users, representing parts of the social network, communicate by using weak connections rather than strong ones. Thanks to the said properties of groups we can focus our analysis on a partition of the social network (where a partition is one or several clusters of users), without loosing consistence and pertinence with the social network in its entireness.

B. Existing online social networks

The main difference between a formal scale-free graph and an online social network is given by the percolation of links [24], i.e. in real life, how worth a certain friend is tends to decrease if there is no good reason to maintain the relationship. This decrease of interest is still true even in a social network, however it has no corresponding support in practice. Such a difficulty on the classification of links results into hard to grip data when performing an automatic analysis. Moreover, in a social network user features change steadily, thus it is difficult to determine the correlation between a user and his/her specific field of interests. Generally, for social networks that let users participate in a group, an average subscriber tends to sign into a large number of groups, while only a small amount of such groups are really interesting for the user.

The said wide-spread user behaviour would be difficult to generalise using traditional approaches, which are not noise robust. In turn, automatic selections and suggestions of posts provided by friends or groups become less useful, because of such inaccuracies. Moreover, it is difficult to distinguish between trustworthy users and dishonest or unreliable ones. Even though the user profile can be potentially genuine, differently from social networks, human networks evolve following a homophily law [25] leading a person to connect with others having similar 'real' interests. Hence, the homophily law lets us detect and reason with small, though relevant, differences between social networks and theoretical scale-free networks. Because of such differences, an existing online social network cannot adhere to a simple mathematical model, instead, since the stochastic behaviour typical of human beings is exhibited, an advanced nonlinear model is needed.

Due to the said untrustworthy, erratic, inconstant and unreliable behaviour of users, we maintain that it is paramount to uncover hidden or un-explicit interests, giving a representation of the effective relationships among users. Such (hidden) relationships are significant to find *categories* of users exhibiting some common traits. Such an identified category would unveil features that can not be directly detected from the user profile.

III. Analytical models

Several generative models can be used to characterise datasets that determine properties and allow grouping data into *classes*. Generative models are based on stochastic block structures [26], on ‘Infinite Hidden Relational Models’ [27], etc. The main issue of class-based models is the type of relational structure that such solutions describe. Since the definition of a class is attribute-dependent, generally the reported models risk to replicate the existing classes for each new attribute added.

E.g. such models would be unable to efficiently organise (inherit) similarities between (from) the classes ‘cats’ and ‘dogs’ as child classes of the more general class ‘mammals’. Such attribute-dependent classes would have to be replicated as the classification generates two different classes of ‘mammals’: the class ‘mammals as cats’ and the class ‘mammals as dogs’. Consequently, in order to distinguish between the different races of cats and dogs, it would be necessary to further multiply the ‘mammals’ class for each one of the identified race. As a consequence, such models quickly lead to an explosion of classes. In addition, we would either have to add another class to handle each specific use or a mixed membership model, as for crossbred species.

Another paradigm concerns the Non-Parametric Latent Feature Relational Model, i.e. a Bayesian nonparametric model in which each entity has boolean valued latent features that influence the model’s relations. Such relations depend on well-known covariant sets, which are neither explicit or known in the case of a social network during the initial analysis.

IV. The multi-agent system

Our aim is to provide to social network administrators a practical and effective tool to predict and monitor user behaviour and interests, both for security purposes and user experience enhancing. Figure 1 shows the agents for our designed system: a *Crawler Agent* periodically and autonomously gathers user information from their social network profiles, other than the list of their group subscriptions. After some preprocessing tasks, data are given to the *Classification Agent* that using the inner RBPNN assigns user profiles to known categories, according to the statistical model built on user information during training phases. Due to the intrinsic dynamics that the social network imposes, this model is constantly and incrementally updated.

The classification results, i.e. the associations between user profiles and categories, are given to the *Verification Agent*, that asks the *Category Agent* to provide the categories already assigned to a specific user (if any), comparing them with the ones just given from the Classification Agent results. If a specific user had no category assigned, the Verification Agent will notify the Category Agent with the newly one found; if instead the user already had a category assigned, but differing from the one just discovered, we could think at this as a clue for an autogenous threat (see Section IV-B) that should be reported to the administrator for further surveys on the user behaviour. This is achieved giving the profile of the threatening user to the *Alert Agent*, that constantly handles all the received notifications, timely warning the administrator with the potentially threats intercepted.

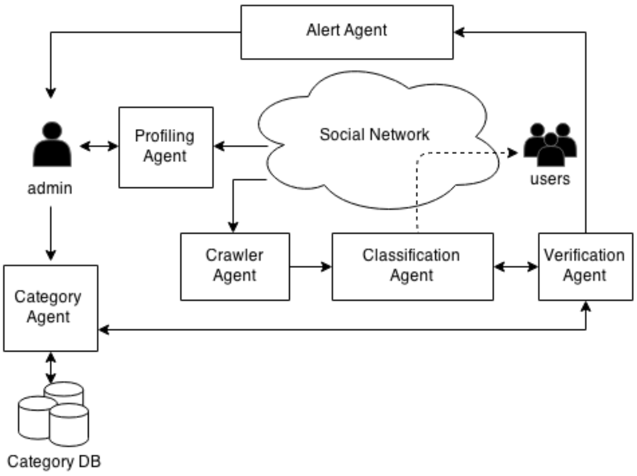

Fig. 1. Schema of the data flow through the agents of the proposed system

The administrator has also the ability to manually define categories built over the activity information of misbehaving users (see Section IV-C); if one of these categories is assigned to a user profile during classification, the Verification Agent will ask the Alert Agent to notify the administrator with the potential threat detected.

The administrator is then able to gather deeper information on the user activities using the functionalities provided by another agent, the *Profiling Agent*. Using this information, s/he can decide what to do according to social network policies. If the user behaviour is considered not compliant with such policies, the administrator has the ability to use the classification information to automatically identify other users in the network with the same behaviour, asking the Classification Agent to update the inner RBPNN model. On the other hand, if the behaviour of the user can be considered trustworthy, then the new classification label can be simply passed to the Category Agent.

Since we can see a *group* of a social network as a category of users, that gets together people with common interests, we can use the same approach just seen to classify user profiles with the groups that better suit their interests. This type of classification results could be directly provided by the Classification Agent as recommendations for groups that user can subscribe to (see Section IV-D).

A. Computing comprehensive identities

User categories can be chosen by the Classification Agent alone, which is statistically driven, and such categories have a probabilistic meaning that contributes to identify the most appropriate conceivable model for users. The ‘model’ should be intended as a kind of representation of the behaviour of a user on the social network. The identified category, provided by the inner RBPNN classifier, can complement and integrate the online identity provided by each subscriber.

Such a comprehensive identity, assigned automatically, can help further understanding user behaviours. To make this solution as independent as possible from the social network data infrastructure, we store and manage additional data with a further agent, that is the Category Agent, but where a more integrated solution is desirable (and conceivable), we can imagine to add such data directly inside the social network user profiles. Once a user belongs to a given category, the administrator can be warned by the Alert Agent to check whether the subscribers linked to a category of misbehaving users are performing activities that conflict with social network policies. When a user posts a content or subscribes to a group, the social network administration is aware of the implicit or explicit choices made beforehand by that user. This 'history' helps understanding whether the current user activity is coherent or appropriate.

Data are continuously sent to the Classification Agent, hence tentative categories identified for a new user are either confirmed or changed according to the recent activities. Hence, more refined alert are given over time.

B. Preventing deception and threats

Theoretically, the RBPNN used by the Classification Agent unveils behavioural patterns that the user is expected to follow. If a user begins to act according to a different behavioural pattern with respect to those for which s/he has been classified, then this variation can be used as an alert that let an administrator monitor him/her and possibly apply some restrictions after a deeper check has occurred. Such an alert is meant to reveal a compromised account that has been stolen.

Once a user account has been confirmed as compromised, either manually or automatically, the supporting system can be set to rise a warning toward all the users that are the target of the activities of the perpetrator, in order to possibly avoid tentative deceptions.

Therefore, the proposed Classification Agent can be used to avoid autogenous threats, such as a misbehaving user or a thief, as much as a wide range of other online frauds and several violations. The more online behaviours are modelled, by training the RBPNN model with existing user data, the more positive and negative activities can be identified by the Classification Agent.

C. Security enforcement

Suppose that a user is disposed toward a bad behaviour on the network, then the Classification Agent would associate such a user with a category previously built by administrators, consisting of other misbehaving users. For building such a category, administrators would simply need to manually flag some selected users, interacting with the Category Agent to store these expert supervised associations.

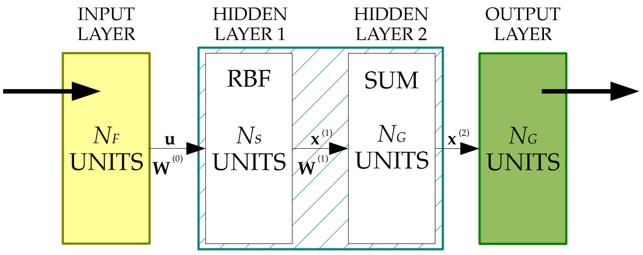

Fig. 2. RBPNN setup values: N_F is the number of considered features, N_S number of analysed subscribers, and N_G desired number of categories.

Although in some moments it would depend on human activities (i.e. administrators), such a control system can then be used to automatically restrict deeper surveys on a small number of possibly dangerous users, so that situations when urgent actions are needed can be timely handled. This automatic selection of users would avert the risk of having to restrain the entirety of subscribers.

D. Group recommendation

Although in this work the RBPNN model has been used to assign categories, which correspond to groups, the term 'categories' has been used on purpose for its more general meaning. The Classification Agent, with its RBPNN model, is able to find and propose non explicit groups, i.e. groups that have not yet been chosen by a subscriber, but which are very likely to be eventually chosen since they match the preferences of the subscriber. In a similar way, this RBPNN can be arranged to select users having an high affinity toward a group. I.e. the RBPNN can be asked to unveil the affinity of a user with a certain category of users, which can be intended not only as a group, but also as a behavioural category.

V. Proposed RBPNN based Classification Agent

Classical models suffer of the incompleteness of the initial input dataset (see Section III). On the other hand, neural networks have been largely used to uncover data classification and find probabilistic categories for data. Therefore, we use Radial Basis Probabilistic Neural Networks (RBPNN), managed by an independent agent, to automatically find *categories* of users, whereby a category reveals common traits for users. Note that *group* of 'ego' networks and social networks, such as Facebook, can be seen as categories, which the RBPNN finds. Our neural network, after being correctly trained, generates a model for the latent user features, and finds users having such features. This is usually considered both an interesting and difficult task [28]. However, the activation functions used for RBPNNs have to meet some important properties required to preserve generalisation abilities and the decision boundaries of Probabilistic Neural Networks (PNN) [29]. The selected RBPNN architecture takes advantage from both PNN topology and Radial Basis Neural Networks (RBNN) used in [30].

In a RBPNN both the input and the first hidden layer exactly match the PNN architecture. In a PNN, each hidden layer neuron performs the dot product of the input vector $\mathbf{u}$ by a weight vector $\mathbf{W}^{(0)}$, and then gives output $\mathbf{x}^{(1)}$ that is provided to the following summation layer. While preserving the PNN topology, to obtain the RBPNN capabilities, the activation function is a radial basis function (RBF). We name f the chosen RBF, so the output of the first hidden layer for the j-esime neuron is

$$\mathbf{x}_j^{(1)} \triangleq f\left(\frac{||\mathbf{u} - \mathbf{W}^{(0)}||}{\beta}\right)$$

where β is a parameter that controls the distribution shape.

The second hidden layer in a RBPNN is identical to that of a PNN, it just computes weighted sums of the values received from the preceding neurons. The training for the output layer is performed as in a classic RBNN, however since the number of summation units is very small and in general remarkably less than in usual RBNNs, training becomes simplified and speed greatly increased.

The devised topology enable us to distribute different parts of the classification task to different layers (see Figure 2). The first hidden layer of the RBPNN is responsible to perform the fundamental task expected from a neural network, i.e. generalise and build an implicit model. The second hidden layer selectively sums the output of the first hidden layer. The output layer fulfils the nonlinear mapping, such as classification, approximation and prediction.

In order to have a proper classification of the input dataset, i.e. of users into categories, the size of the input layer matches the number N_F of *features*, labelled elements of the dataset (see Section VI), given to the RBPNN, whereas the size of the RBF units matches the number of examined subscribers N_S. The number of units in the second hidden layer is equal to the number of output units, these match the number of categories N_G to be found for the subscribers.

VI. Experimental setup

Since the paramount importance of the classification component in the proposed multi-agent solution, we have deeply tested the performance of the conceived RBPNN classifier used by the Classification Agent. We used a dataset consisting of features, i.e. a trace of the user activities and their preferences, coming from real Facebook profiles. Data for the features that we have been given have a label which is a numerical ID, i.e. the feature itself can not be recognised, however this does not affect the scope of this work nor the analysis performed.

As far as the feature lists is concerned, data provide boolean values. The presence or absence of a specific value is expressed as a boolean flag, e.g. 1 if the user has declared his job or 0 if no job information is given in the profile. Among such boolean values there are mutually exclusive values such as the gender, e.g. 1 if male or 0 if female.

The intrinsic structure of the dataset prevents us from considering only a reduced portion of the feature list for a user. A piece of information is usually largely spread over a certain number of features, e.g. a boolean variable could express if the gender is stated or not, and only if stated another variable could report if the user is male or female; then in case the profile does not state the gender, the latter feature has no meaning and should not be considered. However, since our dataset gives no labels, we can not exclude any feature.

Although data are anonymised, users are identified with a unique ID. Moreover, the memberships of users to groups is indirectly identified from the list of subscribers to each group.

Data intended to be input for our RBPNN have been passed to a preprocessing stage, whereby for each user the corresponding feature list has been paired with the list of group memberships. This enables us to build a statistically driven classifier that identifies the correspondence between user features and their groups.

VII. RBPNN findings

Both user profiles, consisting of features, and user memberships to groups were provided to our RBPNN classifier during the training phase. Therefore, the RBPNN classifier has learnt how to reproduce the correct paths that associate lists of profile features with groups.

Initially, we have asked our RBPNN to reconstruct the groups for 250 users. The RBPNN was able to correctly assign users to the proper groups with only a 5.67% of missing assignments: as a remarkable side effect while a few groups were not found, no false positive was given (see Figure 3). Moreover, if we compare the features for such unclassified users and the average features of their groups, relevant differences can be uncovered with respect to the average (and correctly classified) user. Just for validation purposes, we have performed the same comparison for users with an almost empty profile that the RBPNN could not insert into any category.

Then, we have asked our RBPNN to identify categories for new users. In Figure 3 new users are reported in black or green and are assigned to a group they have not expressed preferences in. For an appreciable percentage of users, i.e. about 20%, the proposed RBPNN has indicated a group that (unknown to the RBPNN) users had membership to. Indeed, a relevant number of the other 80% of user profiles is (almost) empty, therefore no classifier, not only our RBPNN, would manage. On the other hand, how many and which features suffice for a user to be classified depend on the model built by the RBPNN (simply counting the number of empty features is ineffective since they are not equally meaningful).

VIII. Concluding Remarks

With the recent growth of social networks usage, a keen interest for privacy and deception has arisen. In [31], authors describe the results of an extensive comparison between two important social networks such as Facebook and MySpace, showing that the interaction of trust and privacy concerns in social networking sites is not yet understood to a sufficient degree. In [32], authors explore the preservation of privacy and propose a novel method to avoid *neighbourhood attacks*. The authors show that anonymised data can be used to answer aggregate queries accurately.

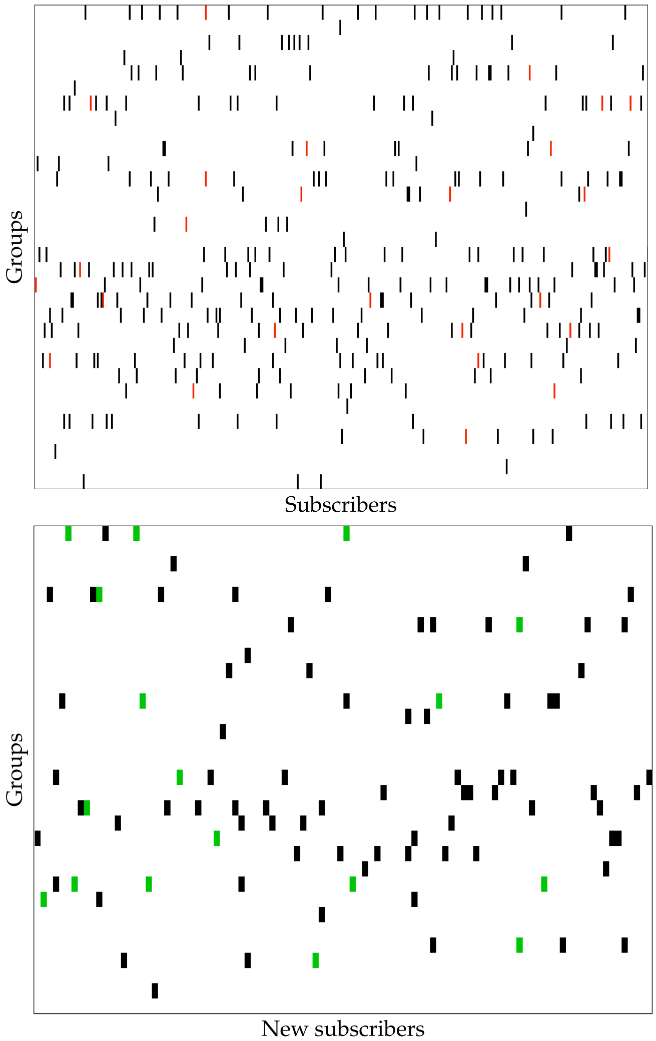

Fig. 3. Top: RBPNN assigned group memberships: correct findings are shown in black, whereas unfound ones are shown in red. Bottom: BPNN assignment to groups for new users: legitimate memberships are in green.

Other previous analyses of data concerning user profiling have taken into account the category of words appearing in texts [33], as well as the user behaviour on-line. The latter solution has been oriented towards an improvement of replica spreading by considering user bandwidth and availability [34]. Moreover, in [35], users have been profiled by observing their interactions with a workflow management system, in a working scenario based on a public administration. All the above profiling strategies can be taken into account and applied into an on-line social network environment for further enriching the classification proposed above.

We have proposed a multi-agent system for automatic analysis of data on a social network and have shown that interesting results can be obtained in terms of the knowledge on the behaviour of users. The proposed solution is based on RBPNN and finds for a user the most similar category (or social network group) s/he could belong to. Once the above solution would possibly be integrated with the servers handling user data, higher security levels could be achieved and the safety of the subscribers would be preserved, e.g. by timely warning administrator to intervene to check and stop autogenous threats.

Acknowledgements

This work has been partially supported by project PRISMA PON04a2 A/F funded by the Italian Ministry of University within PON 2007-2013 framework, and by project PRIME funded by the Italian Ministry of University and Research within POR FESR Sicilia 2007-2013 framework.

References

[1] C. Kiss, A. Scholz, and M. Bichler, “Evaluating centrality measures in large call graphs,” in *Proceedings of IEEE Enterprise Computing, E-Commerce, and E-Services*, 2006.

[2] G. Cybenko, “Approximation by superpositions of a sigmoidal function,” *Mathematics of Control, Signals and Systems*, vol. 2, no. 4, pp. 303–314, 1989.

[3] G. Capizzi, F. Bonanno, and C. Napoli, “A new approach for lead-acid batteries modeling by local cosine,” in *Power Electronics Electrical Drives Automation and Motion (SPEEDAM), 2010 International Symposium on*, pp. 1074–1079, IEEE, 2010.

[4] M. T. Hagan, H. B. Demuth, M. H. Beale, *et al.*, *Neural network design*. Pws Pub. Boston, 1996.

[5] F. Bonanno, G. Capizzi, A. Gagliano, and C. Napoli, “Optimal management of various renewable energy sources by a new forecasting method,” in *Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), 2012 International Symposium on*, pp. 934–940, IEEE, 2012.

[6] M. Woźniak, “On positioning traffic in nosql database systems by the use of particle swarm algorithm,” in *Proceedings of XV Workshop DAGLI OGGETTI AGLI AGENTI - WOA’2014*, vol. 1260, (25-26 September, Catania, Italy), p. paper 5, CEUR Workshop Proceedings (CEUR-WS.org), RWTH Aachen University, 2014.

[7] C. Napoli, G. Pappalardo, E. Tramontana, Z. Marszałek, D. Połap, and M. Woźniak, “Simplified firefly algorithm for 2d image key-points search,” in *2014 IEEE Symposium on Computational Intelligence for Human-like Intelligence*, pp. 118–125, IEEE, 2014.

[8] M. Woźniak and D. Połap, “On some aspects of genetic and evolutionary methods for optimization purposes,” *International Journal of Electronics and Telecommunications*, vol. 61, no. 1, pp. 7–16, 2015. DOI: 10.1515/eletel-2015-0001.

[9] M. Gabryel, M. Woźniak, and R. Damaševičius, “An application of differential evolution to positioning queueing systems,” *Lecture Notes in Artificial Intelligence - ICAISC’2015*, vol. 9120, pp. 379–390, 2015. DOI: 10.1007/978-3-319-19369-4_34.

[10] M. Woźniak, D. Połap, M. Gabryel, R. K. Nowicki, C. Napoli, and E. Tramontana, “Can we preprocess 2d images using artificial bee colony?,” *Lecture Notes in Artificial Intelligence - ICAISC’2015*, vol. 9119, pp. 660–671, 2015. DOI: 10.1007/978-3-319-19324-3_59.

[11] F. Bonanno, G. Capizzi, and C. Napoli, “Some remarks on the application of rnn and prnn for the charge-discharge simulation of advanced lithium-ions battery energy storage,” in *Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), 2012 International Symposium on*, pp. 941–945, IEEE, 2012.

[12] F. Bonanno, G. Capizzi, S. Coco, C. Napoli, A. Laudani, and G. Lo Sciuto, “Optimal thicknesses determination in a multilayer structure to improve the spp efficiency for photovoltaic devices by an hybrid fem—cascade neural network based approach,” in *Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), 2014 International Symposium on*, pp. 355–362, IEEE, 2014.

[13] M. Woźniak, “Fitness function for evolutionary computation applied in dynamic object simulation and positioning,” in *IEEE SSCI 2014: 2014 IEEE Symposium Series on Computational Intelligence - CIVTS 2014: 2014 IEEE Symposium on Computational Intelligence in Vehicles and Transportation Systems, Proceedings*, (9-12 December, Orlando, Florida, USA), pp. 108–114, IEEE, 2014. DOI: 10.1109/CIVTS.2014.7009485.

[14] F. Bonanno, G. Capizzi, and C. Napoli, "Hybrid neural networks architectures for soc and voltage prediction of new generation batteries storage," in *IEEE international conference on clean electrical power (ICCEP)*, pp. 341–344, 2011.

[15] C. Jones and E. H. Volpe, "Organizational identification: Extending our understanding of social identities through social networks," *Journal of Organizational Behavior*, vol. 32, no. 3, pp. 413–434, 2011.

[16] C. Napoli, G. Pappalardo, and E. Tramontana, "A hybrid neuro-wavelet predictor for qos control and stability," in *Proceedings of AIxIA*, vol. 8249 of *LNCS*, pp. 527–538, Springer, 2013.

[17] C. Napoli, G. Pappalardo, and E. Tramontana, "Using modularity metrics to assist move method refactoring of large systems," in *Proceedings of International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)*, pp. 529–534, IEEE, 2013.

[18] C. Napoli, G. Pappalardo, E. Tramontana, and G. Zappalà, "A cloud-distributed gpu architecture for pattern identification in segmented detectors big-data surveys," *The Computer Journal*, p. bxu147, 2014.

[19] F. Bonanno, G. Capizzi, G. Lo Sciuto, C. Napoli, G. Pappalardo, and E. Tramontana, "A novel cloud-distributed toolbox for optimal energy dispatch management from renewables in igss by using wrnn predictors and gpu parallel solutions," in *Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), 2014 International Symposium on*, pp. 1077–1084, IEEE, 2014.

[20] Y.-Y. Ahn, S. Han, H. Kwak, S. Moon, and H. Jeong, "Analysis of topological characteristics of huge online social networking services," in *Proceedings of World Wide Web*, pp. 835–844, ACM, 2007.

[21] A.-L. Barabási, "Scale-free networks: a decade and beyond," *Science*, vol. 325, no. 5939, pp. 412–413, 2009.

[22] M. Granovetter, "The Strength of Weak Ties," *The American Journal of Sociology*, vol. 78, no. 6, pp. 1360–1380, 1973.

[23] S. Schnettler, "A structured overview of 50 years of small-world research," *Social Networks*, vol. 31, pp. 165–178, July 2009.

[24] N. Schwartz, R. Cohen, D. ben Avraham, A.-L. Barabási, and S. Havlin, "Percolation in directed scale-free networks," *Phys. Rev. E*, vol. 66, p. 015104, Jul 2002.

[25] M. McPherson, L. Smith-Lovin, and J. M. Cook, "Birds of a feather: Homophily in social networks," *Annual Review of Sociology*, vol. 27, no. 1, pp. 415–444, 2001.

[26] K. Nowicki and T. A. B. Snijders, "Estimation and prediction for stochastic blockstructures," *Journal of the American Statistical Association*, vol. 96, no. 455, pp. 1077–1087, 2001.

[27] Z. Xu, V. Tresp, K. Yu, and H. peter Kriegel, "Infinite hidden relational models," in *Proceedings of Uncertainity in Artificial Intelligence (UAI)*, 2006.

[28] D. Liben-Nowell and J. Kleinberg, "The link-prediction problem for social networks," *Journal of the American society for information science and technology*, vol. 58, no. 7, pp. 1019–1031, 2007.

[29] S. O. Haykin, *Neural networks and learning machines (3rd Edition)*, vol. 3. Prentice Hall, 2009.

[30] F. Bonanno, G. Capizzi, G. Graditi, C. Napoli, and G. Tina, "A radial basis function neural network based approach for the electrical characteristics estimation of a photovoltaic module," *Applied Energy*, vol. 97, pp. 956–961, 2012.

[31] C. Dwyer, S. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of facebook and myspace," in *Proceedings of Americas Conference on Information Systems*, pp. 339–351, 2007.

[32] B. Zhou and J. Pei, "Preserving privacy in social networks against neighborhood attacks," in *Proceedings of Data Engineering*, IEEE, 2008.

[33] C. Napoli, G. Pappalardo, and E. Tramontana, "An agent-driven semantical identifier using radial basis neural networks and reinforcement learning," in *Proceedings of XV Workshop "Dagli Oggetti agli Agenti"*, vol. 1260, CEUR-WS, 2014.

[34] C. Napoli, G. Pappalardo, and E. Tramontana, "Improving files availability for bittorrent using a diffusion model," in *Proceedings of International WETICE Conference*, pp. 191–196, IEEE, 2014.

[35] G. Borowik, M. Wozniak, A. Fornaia, R. Giunta, C. Napoli, G. Pappalardo, and E. Tramontana, "A software architecture assisting workflow executions on cloud resources," *International Journal of Electronics and Telecommunications*, vol. 61, no. 1, pp. 17–23, 2015.