SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM
TMLAI TRANSACTIONS ON MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE
VOLUME 5 NO 4, 2017
ISSN 2054-7390

Counterterrorism: Privately Clustering A Radical Social Network Data

Jamal Boujmil, N. Tagmouti, N. Raissouni
RS&GIS Lab. Dept. Telecommunications
The National School for Applied Sciences of Tetuan
Tetuan, Morocco
jamal.boujmil@gmail.com, nohatg@gmail.com, nraissouni@uae.ma

ABSTRACT

The tradeoff between the needed or essential gathering and analysis of personal data and the privacy rights of individuals is now an important requirement under any counterterrorism program. The most famous and controversial recent example is the revelation that US intelligence agencies systemically engage in "bulk collection" of civilian "metadata" detailing telephonic and other types of communication and activities, with the alleged purpose of monitoring and thwarting terrorist activity. Differential privacy provides one of the strongest privacy guarantees up to now. In this paper, we present a new provably privacy-preserving algorithm able to identify and take action upon members of the targeted subpopulation. Meanwhile, avoiding compromising the privacy of the patriot subpopulation. It is a new algorithm for search methods which use a new combination of nodes social similarity and differential privacy.

Keywords: differentail privacy; social similarity; privacy preserving

1 Introduction

The conflict between the useful or essential collection andanalysis of data and the privacy rights as a fundamental human right of the citizens is at an historical issue. The controversial recent example is Snowden revelations that US intelligenceagencies systemically engage in mass collection of civilianmetadata. This withthe purpose of monitoring andtracking terrorist activities worldwide.

Existing models for data privacy guarantee only an"all or nothing" flavor: privacy rights are either provided toevery member of a nation, or else it is deemed to be afailure[1]. However, those models are valid only if all the populationmembers have the same privacy right or demand. Facing the cruel terrorist group's activities including "Daesh"and similar groups, privacy rights of related members should be reconsidered. It leads to a serious questions about the balance between protectingthe rights of ordinary citizens, while opting for all necessary meansto avoid terrorism. It means that we have to make a trade-offs between the protection of the civilian privacy right and scarifying it in service of such a societal priority. A recent US National Academies studyconcluded that there are not (yet) technologicalalternatives to bulk collection and analysis of civilian metadata,in the sense that such data are essential in current counterterrorismpractices[1].

DOI: 10.14738/tmlai.54.3204
Publication Date: 15th August, 2017
URL: http://dx.doi.org/10.14738/tmlai.54.3204

Our model tends to explicitly acknowledgesuch trade-offs. Thus we will divide a population to two groups: “Terrorist: T” and “Patriot: P”. This last group is a subpopulation to protect and for which the privacy is guaranteed by law, they are to be contrasted with thefirst subpopulation group, which does not sharethose privacy assurances. The population member status whether he is a “T” or a “P” member is unknown, however it can be discovered basing on costly measures including surveillance or intelligence data exchange.

The model balance’s objective is to give a tool to intelligence agencies to identify and take necessary actions, in a large population modeled in a social, and take appropriate actions on the “T” subpopulation. Meanwhile, privacy assurances for “P” subgroup is guaranteed.

A common “contact chaining” graph search method can be used, since starting from known terrorist “seed” vertices in the social network, neighboring vertices are investigated, in order to identify the “T” subnetwork which is the immediate neighbor of the seed. The main concern of such kind of research methods is that it has access to the vertices and related edges information. This will compromise the privacy of the “P” subgroup.

Our objective is to provide a deliberately “noisy” and privacy preserving version of the search method mentioned above, which will provide the intelligence agency a list of the eventual terrorist in a social network for whom subsequent actions are needed. Meanwhile, privacy rights for the “P” will be guaranteed.

Following are the basis of our model:

i. Social network graph data comprising certain number of private data of each involved individual and which they desire to protect. We assume that the intelligence agency has direct access to this network data, and would like to discover and act upon “T” individuals.
ii. ii) A permanent “tag bit”, which defines the membership status of each individual to “T” or “P” subpopulation is used. It can be checked by the third party agency at certain cost, so, the discovery budget should be considered in order to be minimized by the model. The attribution process of the “tag bit” to each individual is unobservable and we suppose that this classification is done basing on certain investigations conducted by related competent agencies or authorities.
iii. iii) Differential data privacy mathematical model[3] which provide rigorous guarantees of privacy for network’s data for individuals for whom the data privacy is required, meanwhile, it allows the discovery for the “T” subpopulation.

It is crucial to define the “privacy” type we want to protect since that this word comprises many definitions and concepts as per Solove’s taxonomy of privacy[4]. We are concerned with the informational privacy which is based on the quantification of information we can deduct from the output of an analysis related to a protected individual.

2 Key Contribution

We make three key contributions in this paper. First, we introduce a privacy preserving class of graph search algorithm designed to find and identify “T” individuals. Second, the algorithm is based on a new network node similarity method introduced by Yong Li [5] to measure the social similarity between all network nodes.Third, since the social similarity is a kind of private date which concerns the compared nodes, thus our randomized algorithm add noise to the output of this similarity function and construct a

noisy similarity matrix. A contact chaining process will drive the search inside the similarity matrix to define the “T” subpopulation.

This framework is the first works to our knowledge to output an explicit list of protected and targeted subpopulations withqualitatively differing privacy rights basing on social similarity techniques.

3 Related Work

The notion of differential privacy and its usage in the community detection or clustering was developed in a series of papers.In [6], authors find that k-anonymization, when done "safely", and when preceded with a random sampling step, satisfies □-differential privacy with reasonable parameters. Another approach was proposed in [7], to upgrade the one mentioned in [8] which does not satisfy differential privacy. They choose Louvain method as the back-end community detection for input perturbation schemes and propose the method LouvainDP which runs Louvain algorithm on a noisy super-graph. For algorithm perturbation, they design ModDivisive using exponential mechanism with the modularity as the score. Another differential privacy community detection algorithm was presented in [9], where it has implications to private data exploration, clustering, and removal of outliers. Furthermore, they use it to significantly relax the requirements of the sample and aggregate technique, which allows compiling of "off the shelf" (non-private) analyses into analyses that preserve differential privacy. Ahmed et al.[10] propose a privacy preserving mechanism for publishing and clustering social network graph data, which satisfies differential privacy guarantees by utilizing a combination of theory of random matrix and that of differential privacy. Meanwhile, Day et al.[11] investigated the problem of publishing the degree distribution of a graph under node-DP by exploring the projection approach to reduce the sensitivity. They proposed two approaches based on aggregation and cumulative histogram to publish the degree distribution.

Another similar approach to our work is the one presented in [1], where the goal was the development of algorithms that can effectively identify and take action upon members of the targeted subpopulation in a way that minimally compromises the privacy of the protected, while simultaneously limiting the expense of distinguishing members of the two groups via costly mechanisms such as surveillance, background checks, or medical testing

One of the main characteristics of our work is the usage of the social similarity as presented in [5] to output the list of the “T” subpopulation. All the published works up to now uses different network similarity techniques for social recommendation[12] or similar purposes. No one of them use it for a differential privacy community detection purpose. For reference we present here after the main works which used the social network similarity for a community detection purpose. Authors of [13]presented a novel algorithm for community detection that combines network structure with processes that support creation and/or evolution of communities. It identifies leaders, and communities that form around those leaders. It naturally supports overlapping communities by associating each node with a membership vector that describes node's involvement in each community. This way, we can identify nodes that are good followers to their leader, and also nodes with no clear community involvement that serve as a proxy between several communities and are equally as important.

Another measure of similarities between vertices based on random walks was proposed [14] and which has several important advantages: it captures well the community structure in a network, it can be

computed efficiently, and it can be used in an agglomerative algorithm called Walktrap to compute efficiently the community structure of a network. The most important work is the one presented in [5] and which we adopt for our approach. They utilize the concept of information and information loss to measure the node similarity. The whole model is based on this idea that if two nodes are more similar than the others, then the information loss of seeing them as the same is less. The present new method has low algorithm complexity so that it can save much time and energy to deal with the large scale real-world network.

In [15], authors have studied the nearest neighbor search problem in complex network via the development of a suitable notion of nearness.

4 Differential Privacy

Differential privacy has different interpretations[3], it is a formal framework to quantifyto what extent individual privacy in a statistical databaseis preserved while releasing useful aggregate information about the database[16]. It assures privacy guaranteesby requiring the indistinguishability of whether or not anindividual data is in the database following the releaseof information after different query by an analyst. Simultaneously for every individual v's data, and in the same time for any analysis algorithm or query Q that theymight be concerned about, Q is almost no more likely tooccur given that this single individual v's data is used in the computation,compared with if it were replaced by any arbitrarily differententry. It means in a practical way that what an observer or analyst learn about an individual "Amine" (e.g., that "Amine" is in contact with another person Baghdadi, or a group of persons, such as members of "Daesh"radical group) is almost independent of Amine'sconnections, so long as Amine is not herself a member of the "T"population. However, it does not prevent himfrom learning that Amine exists at all. This models a settingin which (for example) a national government has access to anindex of all of its citizens (through birth and immigration records),but nevertheless would like to protect information about theirinteractions with each other[1].

Differential privacy definition is introduced here under. It is oriented for social networks graph dataG where individuals are represented as vertices and the social interaction between them is represented as edges (weighted or unweighted). The information which comprises an edge is a private information to protect.

4.1 Definition 1[3]

An algorithm A is □-differentially private (□-DP) if for all pairs of neighbors graphs G, G' and for every output in the range of A:

$$Pr[A(G) \in S] \leq e^{\square} Pr[A(G') \in S] \quad (1)$$

Network graphs G and G' are neighboring graphs if one can be obtained from other by:

- Adding or deleting one edge from one of them or by arbitrary rewiring of the edges incident to a single vertex: *Edge differential privacy*,
- Adding or deleting a node and its adjacent edges: *Node differential privacy*

The smaller the risk multiplier $e^{\varepsilon}$is, the more guarantees to individual data are assured. Its value is directly related to the value of the privacy parameter or budgetε. Hsu et al.[17] deeply study the "economic" alternatives for choosing ε**.**

4.2 Laplacian mechanism

Since its introduction in [18], the Laplacian mechanism has become the standard technique to let a mechanism or algorithm to achievedifferential privacy and has beenused as the basic building block in a number of works on differential privacy analysis in other more complex problem settings[19]. It is based on the concept of *globalsensitivity* of a function fwhich is defined as:

$\Delta f = \max_{G,G'} // f(G) - f(G')||_1$where the maximum is taken over all pairs of neighboring G, G'. Given a function f and a privacy budget ε, the noise is drawn from a Laplace distribution:

$Lap(\lambda) : p(x| \lambda)=(l/2l)e^{-|x|/\lambda}$where $\lambda= \Delta f /\varepsilon$.

A. Theorem 1: Laplace mechanism[18]
For any function f: G $\rightarrow IR^d$, the algorithm A:

$$A (G) = f(G) + Lap_1(\Delta f /\varepsilon),\ldots, Lap_d (\Delta f /\varepsilon) \quad (2)$$

Satisfies -differential privacy, where $Lap_i(\Delta f/\varepsilon)$ are Laplace variables with scale parameter $\Delta f /\varepsilon$

5 Framework

In this section, we will propose our detail differential approach to output the list of the "T" subpopulation in a social network**.**

Let's considerG as a binary graph representing the connectivity of the social network, and A be the adjacency matrixrepresenting the graph, where $a_{i,j}$is the weight between two different nodes i and j. By assumingthat the graph is undirected, A will be a symmetric matrix,i.e. $a_{i,j}= a_{j,i}$for any i and j.

The first step of our framework is the algorithm 1 called DPSim: Differential privacy social similarity output. It is mainly about calculating the social similarity of the graph G basing on the adjacency matrix A. The key element at this stage is the usage of the new social similarity measure introduced by Yong Li [5] where the basic idea is that if two nodes are more similar than the others, then the information loss of seeing them as the same is less than that of others. We will adopt the proposed algorithm in [5] which output the node similarity measure between two nodes i and j based on the information loss proposed in the same work. The larger value of the algorithm output means higher similarity between the corresponding two nodes. This measure is a critical data to protect against any inference, thus we will opt for a perturbation to each entry of the similarity matrixS. To do that, we will generate a Gaussian random matrix $Q \in IR^{n*n}$and where each entry of Q is sampled independently from another Gaussian distribution $N(0, \sigma^2)$. The value of σis defined in [10] and finally the perturbed similarity matrix Š = S + Q.

The following table describes DPSim algorithm:

Algorithm1 : **DPSim (G, A, σ^2)**

Input:

1) **Social network graph G**
2) **Symmetric adjacency matrix** $A \in IR^{n*n}$
3) **Variance for random noise** σ^2

Output: Randomly perturbed similarity matrix Š

(1) Similarity matrix S = Algorithm (G, A) [5]

(2) Compute a random perturbation matrix Q, with $Q_{i,j} \sim N(0, \sigma^2)$

(3) Compute the randomly perturbated similarity matrix $Š = S + Q$

The second step of the framework is the algorithm 2 called DPSearch. The main idea of the algorithm is that the node which has the high social similarity score with other neighbors nodes in the same network, have the high probability to be in the same class or group of subpopulation with them. It means, if it is a "T" or "P" individual, related similar neighbors with high probability can be in the same subpopulation group. Thus, at this stage, we will use the perturbed similarity matrix Što select at each iteration the seed node with the high social similarity score to query its tag bit and discover to which subpopulation group it belongs. If it is a "T" member, contact chain process consisting of tag bit discovery is initiated for its neighbors.

The following table describes DPSearch algorithm:

Algorithm2 : **DPSearch (Š)**

Input: The randomly perturbated similarity matrix Š

Output: List of "T" subpopulation

Initialization: I = Ø , T = Ø , Count = n

(1) Calculate $Š_i = \sum_{j=1}^{n} Šij$**, for each i= 1,…n**

(2) $V = \{ Š_i / i=1,\ldots, n\}$

(3) While Count ≠ 0

Choose $S_{max} = \sup V = S_{i\,max}$

Count = Count – 1

$V = V \setminus S_{i\,max}$

Query TB(n_i) and I = I $\cup$ **{n_i}**

If TB(n_i) = 1 Then T = T $\cup$ **{n_i}**

Loop

For j = 1,…, n and j ≠ i

If $Š_{ij} \neq 0$ **and** $n_j \notin I$

Then:

Query TB(n_j) and I = I $\cup$ **{n_j}**

If TB(n_j) = 1 Then T = T $\cup$ **{n_j}**

End

End

Algorithm 1 as demonstrated by Kenthapadi et al. in [20]satisfies ε-Differential privacy basing on the following assumptions:$\delta<1/2$, $n\geq2$ and $\sigma\geq(1/\varepsilon)[10(\varepsilon+\ln(1/2\delta))\ln(n/\delta)]^{1/2}$.

6 Experiments and Results

In this section we will introduce our planned approach to demonstrate the effectiveness and performance of our differential privacy searchalgorithm against its competitors. Up to now we are in the algorithm implementation phase, thus related experiments are not yet initiated. It will be a subject of another research paper.

6.1 Dataset

In our experiments we will use four different social network graphs. The first one is a real "snapshot" of twitter social network by DMI-TCAT tool [2]basing on specific key words or hashtags which we set up. In our case, we will capture all twitter accounts which are involved in a radical propaganda around following key words and hashtags for a limited time period: "Raqa", "Daesh", "Halab", "Jabhat Annossra", "Akhbar Asham". Those words or hashtags are chosen basing on specific events related to certain radical groups including Daesh. The tool output the social interaction between two accounts including: number of retweets, number of mentioning, and number of shared / like web pages. The social network will be modeled as following:

- Each account will be considered as a node
- An edge between two nodes will be established if they share one of the following events: retweet, mention, same page like. It is important to mention that each edge will be weighted and the weight between two nodes is the sumup of the retweets, mentioning and shared / like pages [21]

The second social network graphs group comprises three networks from Facebook, Live Journal and Pokec. For Facebook data set, we will consider the one collected by Wilson et al. from Facebook [22]. For both Live Journal and Pokec, they are publically available at SNAP graph library [23], [24]. Those social networks are chosen for the fact that theyshould be large enough to truly represent real online social structure. A small network not only under-represents the social structure, but also produces biased results. Also, the number of edges should be large to reveal the interesting structure of the network. For all three benchmark datasets, the ratio of the number of edges to the number of nodes is between 7 and 20 [10] and for the first one it is about 15.

To fulfill the main assumption of our approach which requires a predefined "Tag bit" to identify an individual membership to "T" or "P" subpopulation, and since the networks we will use do not have this identifiers, so we will opt for Pre-processing phase of those networks. It will help us to generate "Tag bit" for "T" and "P" subpopulation synthetically. We will use the "Infection" process adopted by the author in [25]

7 Conclusion

In this research, we focused on algorithm implementation phase proposing a new differential privacy approach basing on nodes social similarity to output and identify members of a target group "T". Results are highly promising providing strong guarantees about the privacy of the patriot subpopulation "P".

REFERENCES

[1] Kanski, J.J., *Clinical ophthalmology*. 6th edition ed2007, London: Elsevier Health Sciences (United Kingdom). P.952.

[2] Liang, Z., et al., *The detection and quantification of retinopathy using digital angiograms.* Medical Imaging, IEEE Transactions on, 1994. 13(4): p. 619-626.

[3] M. Kearns, A. Roth, Z. S. Wu, and G. Yaroslavtsev, "Private algorithms for the protected in social network search," *Proc. Natl. Acad. Sci. U. S. A.*, vol. 113, no. 4, pp. 913–918, 2016.

[4] S. Kok and R. Rogers, "Rethinking migration in the digital age: Transglocalization and the Somali diaspora," *Glob. Networks*, no. July, 2016.

[5] C. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, no. 2013, pp. 211–407, 2014.

[6] D. J. Solove, "Conceptualizing privacy," *Calif. Law Rev.*, vol. 90, no. 4, pp. 1087–1155, 2002.

[7] Y. Li, P. Luo, and C. Wu, "A new network node similarity measure method and its applications," no. 71271070, pp. 1–12, 2014.

[8] N. Li, W. Qardaji, and D. Su, "On Sampling, Anonymization, and Differential Privacy: Or, k-Anonymization Meets Differential Privacy," 2011.

[9] H. H. Nguyen, A. Imine, and M. Rusinowitch, "Detecting Communities under Differential Privacy," 2016.

[10] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre, "Fast unfolding of communities in large networks," *J. Stat. Mech. Theory Exp.*, vol. 10008, no. 10, p. 6, 2008.

[11] K. Nissim, U. Stemmer, and S. Vadhan, "Locating a Small Cluster Privately," *Proc. 35th ACM SIGMOD-SIGACT-SIGAI Symp. Princ. Database Syst.*, pp. 413–427, 2016.

[12] F. Ahmed, R. Jin, and A. X. Liu, "A Random Matrix Approach to Differential Privacy and Structure Preserved Social Network Graph Publishing," 2013.

[13] W. Day, N. Li, and M. Lyu, "Publishing Graph Degree Distribution with Node Differential Privacy," *Proc. 2016 Int. Conf. Manag. Data*, pp. 123–138, 2016.

[14] Z. Jorgensen and T. Yu, "A Privacy-Preserving Framework for Personalized , Social Recommendations," *Proc. 17th Int. Conf. Extending Database Technol.*, pp. 571–582, 2014.

[15] A. Stanoev, D. Smilkov, and L. Kocarev, "Identifying communities by influence dynamics in social networks," *Phys. Rev. E - Stat. Nonlinear, Soft Matter Phys.*, vol. 84, no. 4, 2011.

[16] P. Pons and M. Latapy, "Computing communities in large networks using random walks," *Comput. Inf. Sci.*, vol. 10, pp. 284–293, 2005.

[17] C. Detection, "Nearest Neighbor search in Complex Network for Community Detection," pp. 1–13, 2015.

[18] S. Oh and P. Viswanath, "The Composition Theorem for Differential Privacy," *Int. Conf. Mach. Learn.*, vol. 37, p. 26, 2015.

[19] J. Hsu, M. Gaboardi, A. Haeberlen, S. Khanna, A. Narayan, and B. C. Pierce, "Differential Privacy: An Economic Method for Choosing Epsilon," *IEEE Comput. Secur. Found. Symp.*, pp. 1–29, 2014.

[20] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating Noise to Sensitivity in Private Data Analysis," *Lect. notes Comput. Sci.*, no. 3876, pp. 265–284, 2006.

[21] Q. Geng and P. Viswanath, "The Optimal Mechanism in epsilon,delta-Differential Privacy," p. 16, 2013.

[22] K. Kenthapadi and A. Korolova, "Privacy via the Johnson-Lindenstrauss Transform," *arXiv Prepr. arXiv …*, no. 1, pp. 1–24, 2012.

[23] F. Ahmed and M. Abulaish, "A Generic Statistical Approach for Spam Detection in Online Social Networks," vol. 36, pp. 1120–1129, 2013.

[24] C. Wilson, B. Boe, A. Sala, K. P. N. Puttaswamy, and B. Y. Zhao, "User Interactions in Social Networks and their Implications," *Eurosys'09 Proc. Fourth Eurosys Conf.*, pp. 205–218, 2009.

[25] L. Takac and M. Zabovsky, "Data Analysis in Public Social Networks," *Int. Sci. Conf. Int. Work.*, no. May, pp. 1–6, 2012.

[26] J. Yang and J. Leskovec, "Defining and Evaluating Network Communities Based on Ground-Truth," *ACM SIGKDD Work. Min. Data Semant.*, pp. 745–754, 2012.

[27] D. Kempe, J. Kleinberg, and É. Tardos, "Maximizing the spread of influence through a social network," *Kdd*, p. 137, 2003.