Nm4 - Report

Aus VroniPlag Wiki

This report is based on the findings of an ongoing plagiarism analysis (date: 30-01-2014). It is therefore no conclusive report and it is recommended to visit the page http://de.vroniplag.wikia.com/wiki/Nm4 for newer findings and further information.

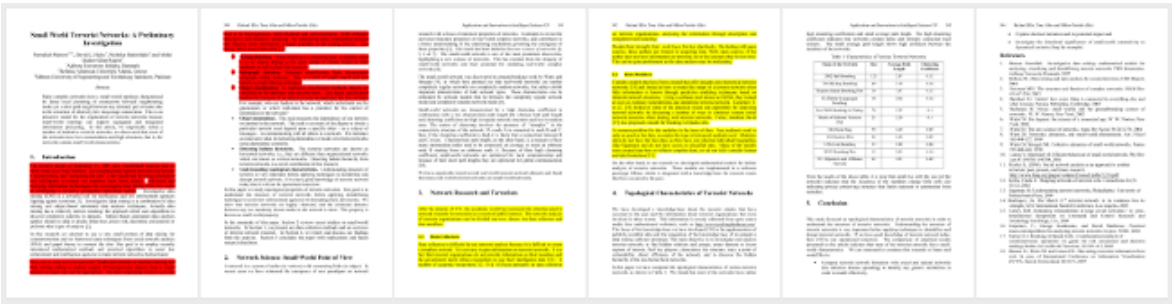
A critical discussion of the publication by Nasrullah Memon, David L. Hicks, Nicholas Harkiolakis and Abdul Qadeer Khan Rajput: *Small World Terrorist Networks: A Preliminary Investigation*

in Ellis, Allen, Petridis eds: Applications and Innovations in Intelligent Systems XV, 339-344, Springer London (2008), →ISBN 978-1-84800-086-5 →Download (http://www.springerlink.com/content/m732505681263247/)

Overview

The following chart illustrates the amount and the distribution of the findings of text parallels. The colours show the type of plagiarism diagnosed:

- rot="Verschleierung": the source of the text parallel is not given, the copied text will be somewhat modified.
- gelb="Bauernopfer": the source of the text parallel is mentioned, but the extent and/or closeness of the copying is not made clear by the reference.



Prominent findings of plagiarism

- Fragment 340 01: A passage is taken verbatim from a source that is not mentioned anywhere in the paper. The authors quote the first author's PhD thesis, which, however, was published after the source.
- Fragment 342 01: A fairly long passage is taken almost verbatim from a source that is named at the end of the passage. However, it is not clear to the reader at all, that the entire passage (in which more references are given) is taken from this source.

Statistics

- Currently there are 5 reviewed fragments documented, that are considered to be plagiarism. For 3 of them there is no reference given to the source used („Verschleierungen“ and „Komplettplagiate“). For 2 fragments the source is given, but the extent of the used text is not made clear („Bauernopfer“).
- The publication has 6 pages that have been analyzed. On a total of 4 of these pages plagiarism has been documented.

This represents a percentage of **66.7%**. The 6 analyzed pages break down with respect to the amount of plagiarism encountered as follows:

Percentage plagiarism	Number of pages
No plagiarism documented	2
0%-50% Plagiarism	3
50%-75% Plagiarism	1
75%-100% Plagiarism	0

From these statistics an extrapolation of the amount of text of the publication under investigation that has been documented as plagiarism can be estimated (conservatively) as **about 25%** of the main part of the publication.

- In all, text was taken from 3 sources.

Duplication

Some of the text of the paper has been presented by the authors previously:

- Section 3 and the beginning of section 4 (p.341: 29-39; p.342: all) can also be found in: Memon et al. (2007c) (retracted)
- Almost the entire section 1 (introduction: p.339: 19-40; p. 340: 1-26) can also be found in: Memon et al. (2007e) (retracted)

References

Memon, Hicks, Larsen (2007c) (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4272050&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4272050) : Harvesting Terrorists Information from Web 11th International Conference Information Visualization (IV'07), 0-7695-2900-3/07 2007 IEEE (retracted)

Memon, Hicks, Hussain, Larsen (2007e) (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4455057&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F4454732%2F4454733%2F04455057.pdf) : Practical Algorithms and Mathematical models for destabilizing terrorist networks in Military Communications Conference, 1-7. MILCOM 2007. IEEE (retracted)

Appendix 1: Fragments

Remark on the colouring

The colouring is automatically generated and shows text parallels. Its purpose is to facilitate the orientation of the reader, it does not, however, automatically diagnose plagiarism of any kind. In order to form a judgement about a certain text parallel one should consult the text itself.

Remark on the line numbering

When identifying a fragment with line numbers everything that contains text (except for the page header and/or footer) is counted, including headings. Usually charts, tables etc. including their captions are not counted, however.

5 gesichtete, geschützte Fragmente

[1.] Nm4/Fragment 339 20

Verschleierung

Untersuchte Arbeit: Seite: 339, Zeilen: 20-25	Quelle: Popp_and_Poindexter_2006 Seite(n): 18, Zeilen: l. col: 1ff	Farbig
The terrorist attacks of September 11, 2001 have transformed America like no other event since Pearl Harbour [sic]. The resulting battle against terrorism has become a national focus, and “connecting the dots” is the watchword for using information and intelligence to protect our countries from future attacks. Advanced and emerging information technologies like investigative data mining offers key assets in confronting a secretive, asymmetric networked enemy.	The terrorist attacks of September 11, 2001 transformed America like no other event since Pearl Harbor. The resulting battle against terrorism has become a national focus, and “connecting the dots” has become the watchword for using information and intelligence to protect the US from future attacks. Advanced and emerging information technologies offer key assets in confronting a secretive, asymmetric, and networked enemy.	

Anmerkungen

The source is not given.

[2.] Nm4/Fragment 339 38

Verschleierung

Untersuchte Arbeit: Seite: 339, Zeilen: 38-40	Quelle: Han_Kamber_2006 Seite(n): 560, 561, Zeilen: 560: last lines; 561: 1ff	Farbig
How can we mine terrorist networks? Traditional methods of machine learning and data mining, taking a random sample of homogeneous objects from a single relation as input may not be appropriate. The data comprising terrorist networks [tend to be heterogeneous, multi-relational and semi-structured.]	*“How can we mine social networks?”* Traditional methods of machine learning and data mining, taking, as input, a random sample of homogenous objects from a single [page 561] relation, may not be appropriate here. The data comprising social networks tend to be heterogeneous, multirelational, and semi-structured.	

Anmerkungen

The source is not given. To be continued on the following page: Nm4/Fragment_340_01.

[3.] Nm4/Fragment 340 01

Verschleierung

Untersuchte Arbeit: Seite: 340, Zeilen: 1-13	Quelle: Han_Kamber_2006 Seite(n): 561, 562, Zeilen: 561: 5ff; 562: 27ff	Farbig

IDM embodies descriptive and predictive modeling. By considering links (relationship between the objects), more information is made available to the mining process. This brings about several new tasks [1]:

- **Group detection.** Group detection is a clustering task. It predicts when a set of objects belong to the same group or cluster, based on their attributes as well as their link structure.
- **Sub-graph detection.** Subgraph identification finds characteristic subgraphs within networks. This is a form of graph search and also known as graph filtering technique.
- **Object classification.** In traditional classification methods, objects are classified on the attributes that describe them. Link-based classification predicts the category of an object not only on attributes, but also on links.

---

1. Memon Nasrullah. Investigative data mining: mathematical models for analyzing, visualizing and destabilizing terrorist networks. PhD dissertation. Aalborg University Denmark, 2007

It embodies descriptive and predictive modeling. By considering links (the relationships between objects), more information is made available to the mining process. This brings about several new tasks. Here, we list these tasks with examples from various domains:

1. Link-based object classification. In traditional classification methods, objects are classified based on the attributes that describe them. Link-based classification predicts the category of an object based not only on its attributes, but also on its links, and on the attributes of linked objects.

[page 562]

7. Group detection. Group detection is a clustering task. It predicts when a set of objects belong to the same group or cluster, based on their attributes as well as their link structure. [...]

8. Subgraph detection. Subgraph identification finds characteristic subgraphs within networks. This is a form of graph search and was described in Section 9.1. [...]

Anmerkungen

The source is not given, instead the author's PhD thesis (see Nm) is quoted, which however has been published after the source.

The copied text begins on the previous page: Nm4/Fragment_339_38

[4.] Nm4/Fragment 341 30

BauernOpfer

Farbig

Untersuchte Arbeit: **Seite: 341, Zeilen: 30-40**	**Quelle: Ressler_2006** **Seite(n): 4, Zeilen: 3ff**
After the attacks of 9/11, the academic world has increased the attention paid to network research for terrorism as a result of public interest. The network analysis of terrorist organizations can be divided into two classes: the data collectors and data modelers.	Since the winter of 2001, the academic world has increased the attention paid to the social network analysis of terrorism as a result of public interest and new grant money.[15] Network analysis of terrorist organizations continues to grow and can be divided into two groups: the data collectors and the modelers.
3.1 Data Collectors	**Data Collectors**
Data collection is difficult for any network analysis because it is difficult to create a complete network. It is not easy to gain information on terrorist networks. It is a fact that terrorist organizations do not provide information on their members and the government rarely allows researchers to use their intelligence data [11]. A number of academic researchers [12, 13 & 14] focus primarily on data collection [on terrorist organizations, analyzing the information through description and straightforward modeling.]	Data collection is difficult for any network analysis because it is hard to create a complete network. It is especially difficult to gain information on terrorist networks. Terrorist organizations do not provide information on their members, and the government rarely allows researchers to use their intelligence data. A number of academic researchers focus primarily on data collection on terrorist organizations, analyzing the information through description and straightforward modeling.
11. Ressler S., (2006). Social network analysis as an approach to combat terrorism: past, present, and future research. http://www.hsaj.org/pages/volume2/issue2/pdfs/2.2.8.pdf 12. Krebs, Valdis E. Mapping networks of terrorist cells. Connections 24 (3) 43-52, 2002 13. Sageman, M. Understanding terrorist networks, Philadelphia: University of Pennsylvania Press, 2004 14. Rodriquez, JA. The March 11th terrorist network: in its weakness lies its strength, XXV International Sunbelt Conference, Los Angeles, 2005	15 See, for example, A. Abbasi and H. Chen, "Identification and Comparison of Extremist-Group Web Forum Messages using Authorship Analysis," *IEEE Intelligent Systems* 20, no. 5 (2005); Kathleen Carley, M. Dombroski, M. Tsvetovat, J. Reminga and N. Kamneva, "Destabilizing Dynamic Covert Networks," in *Proceedings of the 8th International Command and Control Research and Technology Symposium* (Washington, D.C.: War College, 2003); Kathleen Carley, Neal Altman, Boris Kaminsky, Démain Nave and Alex Yahja, "BioWar: A City-Scale Multi-Agent Network Model of Weaponized Biological Attacks," CASOS Technical Report, CMU-ISRI-04-101 (2004); J.A. Rodriquez, "The March 11th Terrorist Network: In its weakness lies its strength," XXV International Sunbelt Conference, Los Angeles, 2005; and Y. Zhou, E. Reid, J. Qin, G. Lai, and H. Chen, "U.S. Domestic Extremist Groups on the Web: Link and Content Analysis," *IEEE Intelligent Systems* (Special issues on artificial intelligence for national and homeland security, forthcoming).

Anmerkungen

The source is given somewhere in the middle and among other references. There is no indication that text has been taken verbatim from the source.

To be continued on the next page: Nm4/Fragment_342_01

[5.] Nm4/Fragment 342 01

BauernOpfer

Farbig

Untersuchte Arbeit: Seite: 342, Zeilen: 1-22	**Quelle: Ressler_2006 Seite(n): 4, 5, 6, Zeilen: 4: 11ff; 5: 9ff; 6: 1ff**
[A number of academic researchers [12, 13 & 14] focus primarily on data collection] on terrorist organizations, analyzing the information through description and straightforward modeling.	A number of academic researchers focus primarily on data collection on terrorist organizations, analyzing the information through description and straightforward modeling. [...]
Despite their strength, their work has a few key drawbacks. By dealing with open sources, these authors are limited in acquiring data. With open sources, if the author does not have information on terrorists, he or she assumes they do not exist. This can be quite problematic as the data analysis may be misleading.	[...]
3.2 Data Modelers	Despite their many strengths, Krebs' and Sageman's works have a few key drawbacks. By dealing with open sources, these authors are limited in acquiring data. With open sources, if the author does not have information on terrorists, he or she assumes they do not exist. This can be quite problematic as the data analysis may be misleading.
Complex models that have been created that offer insights into theoretical terrorist networks [15] and looked at how to model the shape of a terrorist network when little information is known through predictive modeling techniques based on inherent network structures. Using a software tool known as DyNet, they looked at ways to estimate vulnerabilities and destabilize terrorist network. Carpenter, T. et *al.*, [16] looked at some of the practical issues and algorithms for analyzing terrorist networks by discussing a number of ways to construct various social network measures when dealing with terrorist networks. Farley Jonathan David [17] also proposed a model for breaking Al Qaeda cells.	[page 5]
	Modelers
	Complex models have been created that offer insight on theoretical terrorist networks. [...] In a series of projects, Carley and her collaborators deal with a variety of terrorism-related issues. They looked at how to model the shape of a covert network when little information is known, through predictive modeling techniques based on inherent network structures.[19] Using a computational tool created at CASOS known as DyNet, they looked at ways to estimate vulnerabilities and destabilize terrorist networks.[20] [...]
	[...] In addition, in 2002, Tami Carpenter and others began to look at some of the practical issues and algorithms for analyzing terrorist networks by discussing a number of ways to construct various social network measures when dealing with covert networks.[25]
	[page 6]
A common problem for the modelers is the issue of data. Any academic work is only as good as the data, no matter the type of advanced methods used. Modelers often do not have the best data, as they have not collected individual biographies (like Sageman) and do not have access to classified data. Many of the models were created data-free or without complete data, yet do not fully consider human and data limitations [11].	A common problem for the modelers is the issue of data. Any academic work is only as good as the data, no matter the type of advanced methods used. Modelers often do not have the best data, as they have not collected individual biographies (like Sageman) and do not have access to classified data. Many of the models are created data-free or without complete data, yet do not fully consider human and data limitations.
11. Ressler S., (2006). Social network analysis as an approach to combat terrorism: past, present, and future research. http://www.hsaj.org/pages/volume2/issue2/pdfs/2.2.8.pdf	[19] Matthew Dombroski, Paul Fischbeck, and Kathleen M. Carley, "Estimating the Shape of Covert Networks," in *Proceedings of the 8th International Command and Control Research and Technology Symposium* (Conference held at the National Defense War College, Washington D.C., 2003).
12. Krebs, Valdis E. Mapping networks of terrorist cells. Connections 24 (3) 43-52, 2002	[20] Kathleen Carley, "Estimating Vulnerabilities in Large Covert Networks," *in Proceedings of the 2004 International Symposium on Command and Control Research and Technology* (San Diego, CA, 2004).
13. Sageman, M. Understanding terrorist networks, Philadelphia: University of Pennsylvania Press, 2004	[25] Tami Carpenter, George Karakostas, and David Shallcross, "Practical Issues and Algorithms for Analyzing Terrorist Networks" (Telcordia Technologies, 2002).
14. Rodriquez [sic], JA. The March 11th terrorist network: in its weakness lies its strength, XXV International Sunbelt Conference, Los Angeles, 2005	
15. Carley, KM. Estimating vulnerabilities in large covert networks," [sic] in proc. International Symposium on Command and Control Research and Technology San Diego, CA., 2004	
16. Carpenter, T., George Karakostas, and David Shallcross. Practical issues and algorithms for analyzing terrorist networks. In proc. WMC, 2002	
17. Farley D. J. Breaking Al Qaeda Cells. A mathematical analysis of counterterrorism operations (A guide for risk assessment and decision making) Studies in Conflict & Terrorism, 26:399–411, 2003	

Anmerkungen

The source is given at the end of the passage. It is only one of several sources given and the reader does not assume that it is the source of large verbatim text borrowings.

Note that also the publications by Krebs, Sageman and Rodriguez are discussed in the source, however in greater detail.

Appendix 2: Sources

[1.] Quelle:Nm4/Han Kamber 2006

Autor	Jiawei Han, Micheline Kamber
Titel	Data Mining: Concepts and Techniques (second edition)
Ort	San Francisco
Verlag	Morgan Kaufmann, Elsevier
Jahr	2006
Anmerkung	Chapter 9: http://www.cs.uiuc.edu/homes/hanj/cs512/bk2chaps/chapter_9.pdf
ISBN	1-55860-901-6
URL	http://books.google.es/books?id=AfL0t-YzOrEC
Literaturverz.	no
Fußnoten	no

[2.] Quelle:Nm4/Popp and Poindexter 2006

Autor	Robert Popp, John Poindexter
Titel	Countering Terrorism through Information and Privacy Protection Technologies
Zeitschrift	IEEE Security and Privacy
Herausgeber	IEEE Computer Society
Datum	November 2006
Nummer	4 (6)
Seiten	18-27
DOI	10.1109/MSP.2006.147
URL	http://dl.acm.org/citation.cfm?id=1191682; http://www.eecs.harvard.edu/cs199r/readings/popp-sp2006.pdf
Literaturverz.	no
Fußnoten	no

[3.] Quelle:Nm4/Ressler 2006

Autor	Steve Ressler
Titel	Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research
Zeitschrift	Homeland Security Affairs
Herausgeber	Naval Postgraduate School Center for Homeland Defense and Security
Datum	July 2006
Nummer	2 (2)
URL	http://www.hsaj.org/?fullarticle=2.2.8
Literaturverz.	yes
Fußnoten	yes