Proceedings of

CERC2012

Collaborative European Research Conference

26 – 27 April 2012
Darmstadt, Germany

Editors
Patrick Bours
Bernhard Humm
Robert Loew
Ingo Stengel
Paul Walsh

CERC2012

Darmstadt, Germany
26 – 27 April 2012

Proceedings of the

Collaborative European Research Conference 2012

Editors :
Patrick Bours
Bernhard Humm
Robert Loew
Ingo Stengel
Paul Walsh

ISSN : 2220 - 4164

Cover Pictures © Ulrich Mathias
Mathildenhöhe, Wissenschaftsstadt Darmstadt

Table of Content

Chapter 4
Electronic Engineering

Chapter 5
Electrical Engineering

Chapter 6
Civil Engineering

Preface

Interdisciplinary Collaboration is a source of innovation and research. The Collaborative European Research Conference (CERC 2012) is an event to foster collaboration among friends and colleagues across disciplines and nations within Europe. Emerged from a long-standing cooperation between the Cork Institute of Technology, Ireland and Darmstadt University of Applied Sciences, Germany, CERC has this year been extended to include more well-established partners: Plymouth University, UK and Gjøvik University College, Norway.

CERC is truly interdisciplinary, bringing together young researches from science, engineering, business, humanities, and the arts. CERC is innovative, also in the way of creating a real workshop atmosphere. Researchers not only present their findings as published in their research papers. They are also challenged to collaboratively work out joint aspects of their research within conference sessions. Highlights will be presented in a plenary session and the best session presentation will be awarded a price.

To organize such an event involves the hard work of a number of people. Thanks go to the international program committee and my fellow program chairs, particularly to Dr Ingo Stengel for organizing the review process. Dr Robert Loew put a lot of work into preparing the proceedings. He, Janina Fengel, and Prof Udo Bleimann were invaluable for local organization. Thanks also to Prof Bernd Steffensen for supporting CERC, also financially.

Prof. Dr. Bernhard Humm

General Conference & Programme Co-Chair, CERC2012

Darmstadt, April 2012

CERC2012 Committees

General Conference & Programme Co-Chairs

Prof. Dr. Bernhard Humm
University of Applied Sciences Darmstadt, Germany

Dr. Paul Walsh
Cork Institute of Technology, Ireland

Dr. Ingo Stengel
Plymouth University, United Kingdom

Dr. Patrick Bours
University College Gjøvig, Norway

Organizing Committee

Udo Bleimann

Janina Fengel

Bernhard Humm

Robert Loew

Ingo Stengel

International Programme Committee

Shirley Atkinson
Plymouth University, United Kingdom

Udo Bleimann
University of Applied Sciences Darmstadt, Germany

Patrick Bours
University College Gjøvig, Norway

Shun-Ping Chen
University of Applied Sciences Darmstadt, Germany

Nathan Clarke
Plymouth University, United Kingdom

Barry O'Connor
Institute of Technology Cork, Ireland

Tom O'Connor
Institute of Technology Cork, Ireland

John Creagh
Institute of Technology Cork, Ireland

Paul Dowland
Plymouth University, United Kingdom

Klaus-Peter Fischer-Hellmann
University of Applied Sciences Darmstadt, Germany

Orla Flynn
Institute of Technology Cork, Ireland

Steven Furnell
Plymouth University, United Kingdom

Johannes Gerdes
University of Applied Sciences Darmstadt, Germany

Paul Green
Institute of Technology Cork, Ireland

Angelika Groterath
University of Applied Sciences Darmstadt, Germany

Richard Guinee
Institute of Technology Cork, Ireland

Klaus Habermehl
University of Applied Sciences Darmstadt, Germany

Bernhard Humm
University of Applied Sciences Darmstadt, Germany

Chapter 1

Computer Science

Telephony Fraud Detection in Next Generation Networks

S. Augustin, C. Gaißer, J. Knauer, M. Massoth, K. Piejko, D. Rihm, T. Wiens

Department of Computer Science
Hochschule Darmstadt – University of Applied Sciences, Darmstadt, Germany
e-mail: michael.massoth@h-da.de

Abstract

Telephony fraud is a growing problem for telecommunication service providers that operate Next Generation Networks (NGN). This paper describes a framework for a rule-based fraud detection system. The classification of fraudulent calls is based on Call Detail Records (CDR) that are used by telecommunication service providers for billing purposes. By analysing this data, fraud can be detected efficiently. We propose a method for accomplishing this. The work has been conducted in collaboration with a telephony service provider that made real-life CDR data available for analysis. The main achievement of this paper is the description of a rule-based system that detects telephony fraud using CDR data.

Keywords

Communication system security, Communication system signalling, Communication system traffic, Computer network management, Next generation networking

1. Introduction

Telephony fraud is a serious problem for carriers that operate Next Generation Networks (NGN). Attackers regularly try to compromise accounts of users or providers to circumvent charging systems or to cause financial harm to customers. Telephony fraud comprises unauthorized deletion or alteration of billing records, unauthorized bypassing of lawful billing systems, unauthorized billing and the taking of service provider property (Zar, 2005).

1.1. Current situation

The Communications Fraud Control Association (CFCA) estimated in 2009 that fraud leads to a worldwide annual loss of 74 to 80 billion USD (Communications Fraud Control Association, 2009). It is expected that this value will increase in the future. The top three fraud types, as named in their report, are (see Figure 1):

- Subscription or identity theft (22.0 billion USD)
- Compromised Private Branch Exchange (PBX) systems (15.0 billion USD)
- Premium rate service fraud (4.5 billion USD)

Even single fraud attacks may cause significant losses. In one case, an attacker conducted 11,000 calls to Australia, causing an estimated damage of more than 120,000 USD. These calls were made over a period of only 46 hours (Tindal, 2009). These losses could be drastically reduced if effective real-time fraud detection mechanisms were applied.

This kind of fraud also causes significant economic damage because some small- and medium-sized enterprises (SME) may not be able to deal with the amount of financial damage caused by these attackers, possibly leading to bankruptcy.

Figure 1: Top three fraud types

1.2. Challenges in fraud detection

In order to develop well performing fraud detection mechanisms, access to real world data is necessary. However, telecommunication providers are not allowed to expose this data due to privacy reasons. This is caused by national legal limitations, for example the German "Bundesdatenschutzgesetz" (Federal Data Protection Act) (Bundesministerium der Justiz, 2009). Additionally, fraud detection is not just a binary problem. The precise classification of calls as fraudulent or not with a minimum of false positives is difficult. There are cases that cannot be decided with certainty. Therefore, fraud detection has to be treated as an n-class problem (Padmaja, 2007).

1.3. Structure of the paper

This paper is structured as follows: Section 2 gives an overview on the recent activities in the field of fraud detection. Section 3 describes the basic concept of fraud detection and our design decisions for the framework. After the fundamentals have been explained, a more detailed description of our approach is given in Section 4. The paper ends with a conclusion and an outlook on future work in Section 6. Acknowledgements follow in the last section.

2. Related work

In this paper, a rule-based system for fraud detection is described. The field of fraud detection can be divided into multiple categories. Two important ones are rule-based approaches and neural networks. There are also additional approaches, for example Bayesian Networks, Support Vector Machines and Hidden Markov Models. These are described in Section 2.3 (see Figure 2).

2.1. Rule-based methods

Rule-based methods are very effective, but hard to manage. Extensive work is required to specify rules for every imaginable fraud case. Another downside is that rule-based fraud detection systems need to be updated frequently to cover new kinds of fraud (You et al., 2004).

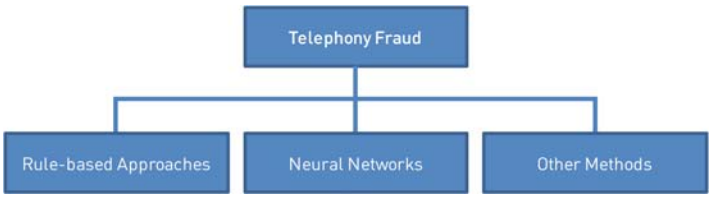

Figure 2: Methods to counter telephony fraud

Rosset et al. (Rosset et al., 1999) proposed an extension of the C4.5 algorithm, which is a popular algorithm to generate decision trees. The extension divides a rule-discovery process into two steps. The first step generates a large number of candidate rules. The second step puts together a rule-set from these candidates. Olszewski (Olszewski, 2011) constructed a detection method based on user profiling by employing the Latent Dirichlet Allocation (LDA). Using the Kullback-Leibler divergence, the participants are classified as "good" or "evil". Ruiz-Agundez et al. (Ruiz-Agundez et al., 2010) propose an architecture for rule-based mechanisms that can be applied in NGN infrastructures.

2.2. Neural networks

One of the alternatives to rule-based approaches for classification are neural networks. These are more suitable to cover new and unknown attacks. Taniguchi et al. (Taniguchi et al., 1998) summarize three methods for fraud detection, one being a neural network. They claim that these three types are able to detect 85% of all fraud cases that occurred in their test set.

1. The first method consists of the application of a feed-forward neural network. It is used to learn a discriminative function to classify service subscribers using summary statistics.

2. The second method applies a Gaussian mixture model to determine the probability of the user's future behavior. This is based on user behavior in the past. The probabilities are used to validate the current behavior in order to detect deviations.

3. The third method uses a Bayesian network. Here, statistical properties of users and of multiple fraud cases are used.

The application of neural networks for fraud detection in mobile communication has been introduced by Qayyum et al. (Qayyum, 2010). A disadvantage of their approach is that further adjustments are needed for the system in order to work efficiently.

2.3. Other methods

The pattern recognition skills of the human eye are very powerful. Therefore, Cox et al. (Cox et al., 1997) proposed to apply humans in the process of fraud detection. They introduced multiple techniques to visualize network traffic in a human readable way. Hollmén and Tresp (Hollmén and Tresp, 1999) proposed a system that is based on a hierarchical regime-switching model. This system receives inference rules from a junction tree algorithm and is trained by using the Expectation Maximization (EM) algorithm.

3. Concept and overall system design

Every internet telecommunication service provider uses charging systems that log each call that was made using the network of the service provider. These log files contain detailed information about calls, and are commonly referred to as Call Detail Records, or sometimes as Call Data Records (CDR). In the CDR, the subscriber numbers of caller and callee, the date and time when the call was made and the call duration are recorded. Therefore, these log files contain valuable information that can be used to detect telephony fraud. Since CDR data is not allowed to be exposed to the public because of German legal regulations, the data provided by the cooperating telecommunication service provider had to be anonymised.

Our system uses CDR files and analyses them for anomalies (see Figure 3). This is accomplished by different filters. Each filter scans the CDRs using specific rules. If an anomaly is detected, and one of the filters supplies a positive result, there is a strong suspicion that a fraud case has occurred. This fraud case has to be validated by a human and further actions, for example the temporary deactivation of an account, have to be taken. Our framework does not automatically perform these actions, as telephony fraud comprises false positives.

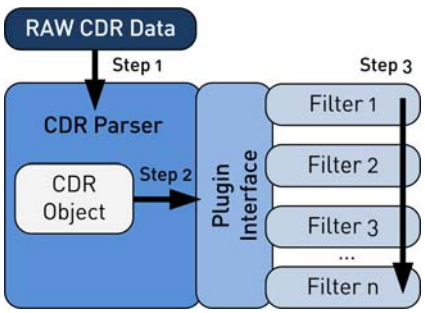

Figure 3: System overview

The framework has been implemented in Python 2.7. The decision to use Python resulted from several considerations. First of all, Python can be learned quickly and, due to its code structure, is easy to read. This ensures a quick start of implementation and results in low costs for later maintenance and the addition of extensions. Furthermore, Python is an open source product that is highly portable and runs on almost every operating system (P. S. Foundation, 2011).

4. System components

In this section, the system components are described in detail.

4.1. Structure of a Call Detail Record

Each CDR consists of several elements that correspond to different functionalities. These elements indicate the start and the end of a call, among other parameters. Each element contains the date and time when the element was written. The first element, indicating the beginning of a record, contains the unique session ID that identifies a CDR. The elements that are necessary for further analysis are now described in more detail.

The Incoming element of a CDR (called A-element in the CDR specification) contains the properties of an incoming call (TELES, 2006). For our purpose, only the carrier ID (the n-attribute of the A-element) is important.

The Connected element (C-element) only exists if a conversation was established. The C-element consists of several sub-elements. For example, its x-element contains the Session Initiation Protocol-(SIP) data of the connection. The SIP data contains several fields. The first field corresponds to the number of the callee. The 13th and 25th field both contain the customer ID or the subscriber number. Furthermore, the C-element includes the duration of a call in milliseconds.

If a call lasts longer than 15 minutes, the CDR is split into multiple parts. These parts can be identified by the first number in the S-element. This element is the first element in a CDR, indicating the beginning of the CDR. If the call duration is below 15 minutes, the identifier is set to ”0”. If it indicates the start of a record series, it is set to ”1”. The final part is marked as ”3”. All parts in between are set to ”2”.

If a call is finished, the Disconnecting element (D-element) is written. In this element, the reason for the call’s termination is stored. The From-field in this element is also important, as it indicates which party hung up. In a nutshell, the C- and the D-element provide the necessary information to bill a call.

4.2. Framework

To analyse the CDRs, we developed a framework that is capable of parsing the log files generated by the billing system. The framework consists of multiple parts:

- Classes for CDRs and CDR-elements parsing the input data.
- The main part of the software controlling the application flow.
- Several filters implementing the rules for fraud detection.

Now, the individual parts of the framework are explained in more detail.

1. CDR Classes: The framework contains classes for each CDR element (see previous section). This modular structure provides easy filter access to the different CDR elements.

2. Main part: This part of the software controls the application flow. It starts the application, evaluates the console commands for the input files that are to be parsed and registers the different filters. The filters are organized as a list, which is iterated for each input CDR. To expand the software, more filters can easily be integrated into the analysis process, simply by adding them to the list of registered filters.

The CDR parser starts to read the data from the given input files. Each CDR is parsed from the log files into a CDR object. Each filter expects a CDR object as input and analyses it. After the input files have been parsed completely, the results from the filters are collected by the main part. If one filter or multiple filters have detected a potential fraud case, the output is saved to a text file. The output contains each filter’s result as a binary value. Then, an operator is alarmed.

The release candidate comes as a console application. A graphical user interface has not been included, since the software is used by the technical staff of the cooperating telecommunication service provider and the systems that process the CDRs are UNIX-based.

4.3. Filters

The framework includes a filter base class that is inherited by all implemented filters (see Figure 4). This base class contains methods for all filters, e.g., for the formatting of date and time, and a method that returns the results. For each rule, which was defined to detect fraud, a filter is implemented. Each filter analyses a given CDR, evaluates it for fraud-suspicious data and returns the collected results to the main class.

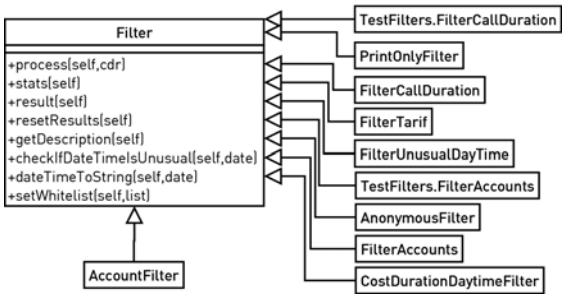

Figure 4: Filter base class and inherited classes

In general, all filters only regard calls originating from the internet telecommunication service provider's network, as only these calls are charged. These are identified if the callee's subscriber number corresponds to a customer ID and the carrier ID in the Incoming element of the CDR does not correspond to the service provider's ID.

Up to date, four filters have been developed. The first filter regards only single calls of a customer. The second one regards all calls of a specific customer per hour. The third filter scans for signalling errors and suppressed caller IDs, while filter number four considers historical user data.

The first filter analyses a single call for the following criteria:

- The duration of the call, depending on the destination pay scale area.
- The date and time when the call was made.

To classify the pay scale area, the destination area code of the callee's subscriber number is analysed. We defined four categories of pay scale areas:

1. No charges: The first category classifies calls that only cause low charges or none at all. Therefore, these calls are omitted. As the software was developed in cooperation with a German company, the relevant area codes include the German fixed network, Voice over Internet Protocol (VoIP) and national subscriber numbers.

2. Moderately expensive: This category comprises calls destined for the German mobile network. These calls are not very expensive, regarding the charges per minute. In this case, calls lasting for more than a specific threshold are considered unusual.

3. Expensive: To simplify the classification, this category includes all calls that do not belong to one of the other categories. These are calls that are destined for international and special rate numbers. A threshold for the call duration is set accordingly.

4. Very expensive: Satellite calls belong to the most expensive category. These calls may be charged at up to 20 per minute. Therefore, the threshold in this category is considerably lower than the thresholds in the previous categories. The second criteria for this filter are the date and the time when the call took place. If, for example, a company only has business customers, it can be assumed that calls outside the business hours or on weekends are more suspicious than others.

The second filter regards all calls that are made by a specific customer in a given time frame. The criteria are as follows: If the amount of calls per hour is greater than a specific value or if the overall call duration per hour exceeds a specific threshold, it is assumed that this is a fraudulent usage of the telephony service.

The first and the second filter also include a whitelist for specific customers. Whitelist candidates are customers who would regularly be above the thresholds with their normal call behaviour, and therefore would be considered as fraudulent. Those customers are maintained in the whitelist and are ignored by the filters.

The third filter scans the input data for signalling errors and suppressed caller IDs, since these may also denote fraud cases. These parameters are only considered for analysis if they are found on incoming calls. Additionally, data in the CDRs indicating the connection quality is assessed by this filter. One of the typical fraud scenarios consists of routing calls via multiple international service providers. In these cases, connection quality may drop significantly. Therefore, low connection quality may be another indicator for fraud cases.

The fourth filter collects historical user data, for example the total duration of calls made by a single user or by all users. Here, up to seven categories may be included. Additionally, this filter is able to output descriptive statistics and diagrams as a PDF file.

Another interesting information contained in a CDR is the reason for call termination. This is stored in the D-element. Among the possible reasons, SIP-signalling errors and identity errors are the most interesting ones from the perspective of fraud detection. These reasons can also be used for statistical purposes or to detect internal network errors.

The filter rules and their associated thresholds have been determined by a thorough evaluation of actual fraud cases. This has been actively supported by the collaborating service provider. Unfortunately, it is not possible to describe the rules and thresholds in more detail. A publication of these parameters would give attackers a significant advantage in bypassing the system, which is productively used.

5. Conclusion and future work

In general, the presented rule-based approach for detecting telephony fraud is promising. The described solution performs well on the real-life CDRs delivered by the service provider, regularly classifying about 4% as false positive fraud cases. Additionally, it is almost an order of magnitude faster than the solution previously used, which was script-based. For example, the presented system is able to process typical CDR files in significantly less than one minute, while the old system took more than ten minutes to accomplish this, under identical circumstances. Furthermore, the system did not only detect known fraud attacks, but also discovered yet unknown SIP-signalling errors that were caused by other carriers. Future work will comprise an investigation of these SIP-signalling errors, since they appear to be potential predictors for telephony fraud. This especially concerns so-called inter-carrier fraud.

Still, the developed system needs more testing. It appears that the thresholds have to be specified more precisely. As these values rely on experiences, the software has to be run in a productive environment with near real-time data to exactly determine the thresholds, in order to increase the detection probability. The final decision, if the results detected by the system are fraud, still relies on a human operator judging each case. Much harm could be done by automatically blocking innocent customers due to false positive classification results. With the presented approach, our system is able to conduct most of the analysis necessary to detect fraud by itself. Therefore, the probability that the delivered results indicate real fraud cases is already high. Given the modular implementation, the system can be easily extended. More rules, that is to say more filters, can be integrated with no effort. The more distinct the filters are that analyse the incoming data, the more likely it is to detect fraud before too much damage is done.

Granted that the presented system is tested more thoroughly, it will be capable to be used on a Next Generation Network for high-performance fraud detection. Its application will possibly improve the detection of telephony fraud, and it is worth considering for use by telecommunication service providers.

It should be stressed that the solution is specifically tailored to the needs of the collaborating service provider. From their perspective, the presented approach represents a major achievement concerning fraud detection in their practice, compared to the previously used solution. In comparison to the related work that has been presented in Section 2, our approach is especially distinguished by its ease of use in relation to the obtainable detection rate. The latter is already sufficient for this special case of application. For the expert personnel that actually use our system, defining or adjusting the rules is intuitive and relatively straight-forward to do. In this regard, our solution differs from other, more general applications of rule-based approaches. Neural networks, on the other hand, are often regarded as non-intuitive, because the inner structure of a trained neural network is not easily interpretable (Hastie, Tibshirani and Friedman, 2008). Hence, adjusting such a system could be harder for the intended users to do. On the other hand, future work will

especially comprise the integration of other methods from the field of machine-based learning into our solution, while keeping the focus at user-friendliness.

6. Acknowledgment

This work has been performed for the “Fraud Detection” project of Hochschule Darmstadt - University of Applied Sciences. The project is partially funded by the “Bundesministerium für Bildung und Forschung” (BMBF) and supported by the ”Center for Advanced Security Research Darmstadt” (CASED). The authors additionally would like to acknowledge the support of toplink GmbH, which made this work possible.

7. References

Bundesministerium der Justiz (2009), “Bundesdatenschutzgesetz“ in der Fassung vom 14. Januar 2003, zuletzt geändert am 14. August 2009,“ Berlin.

K. C. Cox, S. G. Eick, G. J.Wills and R. J. Brachman (1997), “Visual data mining: Recognizing telephone calling fraud,” in: *Data Mining and Knowledge Discovery*, vol. 1, no. 2, pp. 225–231.

Communications Fraud Control Association (2009), “2009 global fraud loss survey,” http://www.cfca.org/, (Accessed 01 September 2011)

T. Hastie, R. Tibshirani and J. Friedman (2008), *The elements of statistical learning*, 2nd edition, Springer, Berlin/Heidelberg.

J. Hollmén and V. Tresp (1999), “Call-based fraud detection in mobile communication networks using a hierarchical regime-switching model,” in: *Proceedings of the 1998 Conference on Advances in Neural Information Processing Systems 11 (NIPS 1999)*. Morgan Kaufmann, 1999; pp. 889–895.

Y. Kou, C.-T. Lu, S. Sirwongwattana and Y.-P. Huang (2004), “Survey of fraud detection techniques,” in: *Proceedings of the 2004 IEEE International Conference on Networking, Sensing and Control (ICNSC 2004)*. IEEE, 2004; pp. 749–754.

D. Olszewski (2011), “Fraud detection in telecommunications using Kullback-Leibler divergence and latent Dirichlet allocation,” in: *Proceedings of the 10th International Conference on Adaptive and Natural Computing Algorithms (ICANNGA 2011)*. Springer, 2011; pp. 71–80.

T. Padmaja, N. Dhulipalla, R. S. Bapi, and P. R. Krishna (2007), “Unbalanced data classification using extreme outlier elimination and sampling techniques for fraud detection,” in: *Proceedings of the 15th International Conference on Advanced Computing and Communications (ADCOM 2007)*. IEEE Computer Society, 2007; pp. 511–516.

P. S. Foundation (2011), “Python programming language - official website”, http://www.python.org, 1990-2011, (Accessed 12. 12. 2011)

S. Qayyum, S. Mansoor, A. Khalid, K. Khushbakht, Z. Halim and A. Baig (2010), “Fraudulent call detection for mobile networks,” in: *Proceedings of the 2010 International Conference on Information and Emerging Technologies (ICIET 2010)*. IEEE, 2010.

S. Rosset, U. Murad, E. Neumann, Y. Idan and G. Pinkas (1999), “Discovery of fraud rules for telecommunications challenges and solutions,” in: *Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 1999)*. ACM, 1999; pp. 409–413.

I. Ruiz-Agundez, Y. Penya and P. Garcia Bringas (2010), “Fraud detection for voice over ip services on next-generation networks,” in: *Proceedings of the 4th Workshop in Information Security Theory and Practice (WISTP 2010)*. Springer, 2010; pp. 199–212.

TELES (2006), “Teles.icdr, S48-S2000 series,” Teles Communication Systems, 2006.

M. Taniguchi, M. Haft, J. Hollmén and V. Tresp (1998), “Fraud detection in communication networks using neural and probabilistic methods,” in: *Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 1998)*. IEEE, 1998; pp. 1241–1244.

S. Tindal (2009), “VoIP hackers strike perth business,” ZDNet, Jan. 2009. http://www.zdnet.com.au/voip-hackers-strikeperth-business-339294515.htm, (Accessed 05 August 2011)

Zar, J. et al. (2005), "VOIPSA - VoIP security and privacy threat taxonomy, public release 1.0", http://www.voipsa.org/activities/taxonomy.php, October 2005, (Accessed 05 August 2011)

A Criteria-Driven Method for Architecting Domain-Specific IE Applications

T. Neef, S. Morana, B. G. Humm

Department of Computer Science
Hochschule Darmstadt – University of Applied Sciences, Darmstadt, Germany
{tobias.neef, stefan.morana}@stud.h-da.de, bernhard.humm@h-da.de

Abstract

This paper proposes a method for architecting domain-specific information extraction (IE) applications focusing on a good cost/benefit ratio for a concrete domain. The method uses criteria to recommend the appropriate use of rule-based or machine learning based methods in the IE application architecture. By using an example from the tourism domain, the paper describes how the evaluation criteria can be applied in practice. An evaluation of the costs and benefits indicates a good IE recognition rate with reasonable development effort.

Keywords

NLP, supervised Information Extraction, tourism, architecture

1. Introduction

Companies have increasing need to access semantic information contained in natural language text. This is an ongoing trend in the last decade which is mainly motivated by the fact that the Internet enables companies to access massive amounts of information available in textual form. Semantic information in the context of this paper is knowledge contained in documents which are relevant to users of a specific domain. *Natural Language Processing (NLP)*, and in particular *Information Extraction (IE)* is the technique to extract semantic information from natural language text. A profit-oriented institution that develops an IE application needs to define a domain-specific architecture with a good cost/ benefit ratio.

Most IE publications, today, focus on approaches which solely increase the recognition rate, i.e., the benefit of IE applications. However, the development costs induced by those approaches are rarely considered. In this paper, we define a criteria-driven method for specifying the architecture of domain-specific IE applications with a well-balanced cost / benefit ratio.

The paper is structured as follows. Section 2 presents related work including state-of-the-art domain-specific IE approaches. Based on these approaches, the method for architecting domain-specific IE applications is defined (Section 3) and then applied to a specific domain (Section 4). The evaluation (Section 4.3) shows the development effort (cost) and recognition rate (benefit) of the resulting application. Section 5 concludes the paper.

2. Related Work

Recent work has shown the capabilities of various approaches for IE in domain-specific (supervised) scenarios. Those approaches can be categorized into two logical components, *Entity Mention Detection (EMD)* and the *Relation Mention Detection (RMD)* (Surdeanu et al., 2011). EMD groups the techniques used for detecting (named) entities. RMD detects (semantic) relations which connect entities.

Publications like (Surdeanu et al., 2008) and others focus on applications which are solely based on *Machine Learning (ML)*. In ML, the extraction of information is based on an ML model which was trained with sample data, a so-called *corpus*.

IE systems like ANNIE (Isabelle et al., 2001) do not use machine learning. Instead, the system relies on domain-specific resources like gazetteers or taxonomies for EMD. ANNIE is capable of doing morphologic normalization and basic rule-based co-reference resolution in order to increase the entity recognition rate. Extended versions of ANNIE use the annotation pattern language JAPE which is a finite state transducer (Cunningham et al., 2000). With JAPE, rules can be defined which use syntactic information to realize rule-based EMD and RMD. (Wyner and Wim, 2011) shows how this

approach is applied to the legal domain. They propose a linguistically motivated system which is based on Phrase Structure Parses to represent syntax.

(Surdeanu et al., 2011) argue that in supervised scenarios, the performance of a domain-specific IE application can be optimized using domain-specific components like rules and gazetteers.

In summary, both ML-based and rule-based approaches as well as mixed approaches have been applied to domain-specific IE. The focus of research in those areas was on the improvement of recognition rate measures. The following section proposes evaluation criteria which also consider the effort spent on learning and customizing a system.

3. A Criteria-Driven Method for Architecting Domain-Specific IE Applications

3.1. Overview

The method takes as input the prioritization of certain criteria and influencing factors of the problem domain. The outputs are architecture recommendations for the IE application to be constructed. See Figure 1.

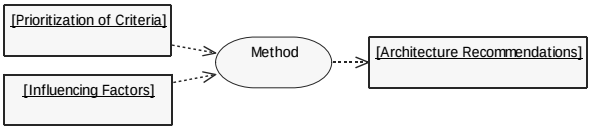

Figure 1: Inputs and outputs of the method

Criteria, influencing factors and architecture alternatives are described in the following sections.

3.2. Criteria

General criteria for architecting applications are *costs* and *benefits* where a good cost / benefit ratio is aspired. In the context of IE applications, these criteria can be refined as follows.

1. *Recognition rate*: a high recognition rate is the main benefit of an IE application

2. *Effort*: the development effort is the main cost factor for an IE application and should be as low as possible. It can be split up into two factors.

    2.1. *Customization effort:* IE applications are usually built on top of off-the-shelf IE components that need to be customized. The classic programming effort is usually relatively low.

    2.2. *Learning effort:* The use of off-the-shelf IE components is usually complex and requires proficiency in NLP and the technique used. Depending on the NLP expertise in the development team, the learning effort may be substantial.

In this paper, we do not consider the cost factor for software licences since our method is independent of concrete off-the-shelf products and their pricing models.

Depending on the domain under consideration, either criterion may be prioritized differently. In one project, the recognition rate has top priority and high costs may be acceptable. In other projects, a reasonable recognition rate is acceptable but the costs must be limited. The *prioritization of the criteria* is an important input for architectural decisions.

3.3. Influencing Factors

Apart from the prioritization of the criteria, there are other factors influencing architectural decisions for IE applications.

1. *Linguistic complexity*: the domain under consideration may involve different linguistic complexities. Aspects are, e.g., grammatical correctness incl. the occurrence of typing errors, the use of domain-specific terminology, the writing style (length of sentences, nesting depth), or the occurrence of co-references.

2. *Team expertise*: The expertise of the development team regarding NLP and IE technologies and concrete off-the-shelf components has a strong influence on the learning curve and the development effort.

3. *Domain-specific resources*: The availability of domain-specific resources like, e.g., dictionaries (taxonomies, ontologies) or corpora has an influence on IE approaches to be used.

3.4. Reference Architecture for IE Applications

Figure 2 shows a reference architecture for IE applications, i.e., a blue print that shows essential components, inputs and outputs of IE applications in general.

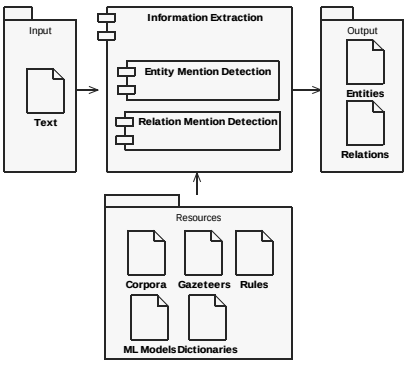

Figure 2: Reference architecture for IE applications

The main *input* for an IE application is *text* in a natural language. The main *outputs* are detected *entities* and *relations*. The main components of an IE application refer to the main *IE tasks*: *Entity Mention Detection (EMD)* and *Relation Mention Detection (RMD)*. *Resources* may be used to configure the IE components: *corpora, ML models, gazetteers, dictionaries*, and *rule sets*.

EMD and RMD may be performed by both, *machine learning (ML)* and *rule-based (RB)* approaches each using different resources. See Table 1.

IE Approaches **IE Tasks**	**Machine Learning (ML)**	**Rule-Based (RB)**
Entity Mention Detection (EMD)	Corpora, ML Models (Gazeteers, Dictionaries)	Rules, Gazeteers, Dictionaries
Relation Mention Detection (RMD)	Corpora, ML Models	Rules

Table 1: Resources used by IE approaches for IE tasks

3.5. Architecture Recommendations

Our method gives architecture recommendations for IE applications depending on the prioritization of criteria and influencing factors of the domain under consideration. The following Table 2 gives an overview.

Topic	Input: Prioritization of criteria and influencing factors	Architecture Recommendation			
		EMD		RMD	
		ML	RB	ML	RB
(A.) Prioritization of criteria	(A.1) Top priority on recognition rate	✓		✓	
(B.) Linguistic complexity	(B.1) High linguistic complexity	✓		✓	
	(B.2) Low linguistic complexity		✓		✓
(C.) NLP expertise	(C.1) Limited NLP expertise in development team		✓	×	✓
	(C.2) High ML experience in development team	✓		✓	
	(C.3) High linguistic experience in development team		✓		✓
(D.) Domain-specific resources	(D.1) Dictionary available	✓	✓		
	(D.2) Annotated corpus available	✓		✓	

Table 2: Overview of architecture recommendations

The column "Input" describes the prioritization of criteria and influencing factors in a particular application domain. The column "Architecture Recommendation" indicates a preferable selection of an IE approach (machine learning or rule-based) for a particular IE task (entity mention detection or relation mention detection). A tick (✓) denotes a suitable approach, a cross (×) denotes an approach which is to be avoided. If, in a concrete application domain, different recommendations are in conflict then the application architect has to make an informed decision. The following paragraphs will help the architect in making such a decision.

Basics

Named entity recognition (NER) based on gazetteers can be broken down into two segments. The first one includes pre-defined lists of categorized words *(gazetteers)*. If there is no doubt to which category those lookups belong to then they can be marked as Named Entities. Often, it depends on the context of a token to which category the Named Entity can be assigned. Also problems like word sense ambiguity, incorrect spelling or co-references make it unfeasible to solely rely on gazetteer lists. Therefore, gazetteer-based systems like ANNIE include context-specific rules in order to yield better EMD performance.

Another approach to EMD is the use of machine learning (ML) based NER as pioneered by (Lafferty, 2001). As with all ML approaches, a vast amount of pre-annotated documents of the given domain have to be available to yield good results. But those systems can be significantly more robust against various forms of misspellings. Additionally, they can learn the correct categorization for the given context and they already solve some co-reference related problems.

When evaluating the complexity of both approaches it soon becomes obvious that the complexity characteristics are not linear. Instead they are a function based on the quality of input data which is available for a given domain, and on the linguistic complexity of the domain.

Linguistic Complexity (B.)

The rules in a RB approach have to be created manually. The customization effort for the system increases with the linguistic complexity of the domain documents. A ML-based application uses a corpus. The complexity of annotating a corpus is not related to the linguistic complexity of the document. As a consequence, we recommend ML-based approaches for EMD and RMD when the linguistic complexity is high (B.1).

Prioritization of criteria (A.)

Rule-based and ML-based approaches can also be combined. According to (Surdeanu et al., 2011), the combination of gazetteers and ML-based NER is required to optimize the recognition rate of a domain-specific IE application. However, this combination has an effect on the system complexity and, hence, on learning and customization effort. If the recognition rate is prioritized (A.1) then the combination of ML-based and RB approaches is recommended.

Domain-specific resources (D.)

In the gazetteer approach, gazetteer may be derived from resources like dictionaries or taxonomies. If such resources do not exist then domain-specific gazetteer lists need to be constructed manually by domain experts. Depending on the domain and the number of relevant entities, this may lead to a customization effort which is not acceptable anymore (Kozareva, 2006) (D.1).

The initial customization effort of the ML-based NER is mainly influenced by the effort required to annotate documents. They are the input for the learning algorithms. If those annotated documents are not available then the effort of creating a sufficiently large corpus of good quality is a high initial investment.

When looking at the customization effort of both approaches we argue that gazetteer-based applications have a relatively low initial customization effort. It increases if the quality of the domain specific dictionaries is low or no dictionaries are available. The initial customization effort of ML based methods is higher but does decrease when an annotated, similar corpus is already available (D.2).

NLP Expertise (C.)

The learning effort of the gazetteer-based approach is mainly related to the linguistic complexity of the domain and the annotation features available. The learning effort of creating gazetteer lists is minimal as long as the creator of the lists has enough domain knowledge. In contrast, the EMD related rules require a solid understanding of rule systems like JAPE (Cunningham, et al., 2000), as well as the features which are used as input for the rule system. Features can be part-of-speech (POS) information as well as various representations of syntax.

The learning effort of ML-based NER is mainly influenced by the abstractions the tools offer to hide the complex ML algorithms from the developer. This has been a problem which was actively worked on since research started to focus on this area (Lafferty, 2001). Therefore, tools have emerged on the market like the Stanford NER (Finkel, et al., 2005) or GATE's Batch Learning PR (Li, et al., 2005) which are useable for an average developer to create a domain-specific NER models.

An important factor in the learning effort of the EMD component is the background of the developers. If they have a more linguistic background the gazetteer based approach is recommendable (C.3). When the users have some background in statistics and machine learning, they can soon get productive with the ML-based approach (C.2). Both techniques have a certain level of initial complexity which needs to get resolved.

In ML-based RMD, features like Named Entities are required which are detected by preprocessing steps or EMD. Those features and a corpus annotated with relations is the input for a learning algorithm. The combination of these features and the customization is an expert task and, from our perspective, no tool has gained enough traction to be used outside a specific research group (C.1).

Rule-based RMD is mostly based on syntax information. This information is then processed by a rule system in order to find the semantic relationships. There are two commonly used syntactic representations: *phrase structure parses* and *dependency grammars*. Phrase structure parses are trees that are optimized to represent the syntax in a detailed and linguistically correct way. Therefore, it has been used in many systems in the past. Publications like (de Marneffe and Manning, 2008) showed that for most non-linguists the dependency grammar representation is more appealing. They also proposed a dependency representation which is mainly motivated to provide semantically helpful information instead of showing all the syntactic details. Our experiments indicate that the acceptance of the dependency-based syntax representation is higher than the phrase structure parses for developers without a linguistic background. Further evaluation criteria of syntactic parsers and their representation have been developed by (Miyao et al., 2008).

Although the same customization effort tradeoffs apply for ML-based RMD as they do for EMD, we argue that, due to the lack of tool support in the ML-based RMD area, the learning effort and is too high to recommend the approach.

4. The Method Applied in a Sample Domain

4.1. The Hotel Domain

In order to demonstrate the proposed method, we introduce an IE problem in the tourism domain. This IE task was accomplished within the research project "Ontology-Based Text Mining" (OBTM) at Hochschule Darmstadt – University of Applied Sciences for the company HRS – Hotel Reservation Service, a leading hotel portal provider in

Germany. The task was to extract information about a hotel, its properties, and also about it rooms and their equipment. Thousands of textual hotel descriptions are available in catalogues or online web pages. HRS plans to use this information for offering their customers better search capabilities. In order to achieve this goal, a semantic understanding of natural language text is required. The OTA code list (OpenTravel Alliance, 2010), which is an existing classification system for the tourism domain, defines categories of hotel-related entries. All terms in the OTA code list have an identifier.

Code	Name	Category
GRI42	Room	Accommodation Profile, Accommodation Unit
HAC79	Sauna	Hotel Facility, Unit Facility

Table 3: Examples of OTA codes and categories

Hotel codes are assigned to categories depending on their roles. For example, the code "GRI42/Rooms" may be used to indicate the total amount of rooms. In the hotel description, this fact may be formulated as follows.

> "Our hotel has 120 well-equipped rooms."

In this case, it is expected to find a relation between the code "Room" and the number 120 which quantifies it.

> RoomAmountRelation(GRI42/Room, 120)

Another role of a room is an Accommodation Unit which includes so called "Unit Facilities".

> "All our rooms contain a sauna for your personal pleasure."

In this case it is expected to find relationships between the room and the units which are contained in this room.

> RoomUnitRelation(GRI42/Room, HAC79/Sauna)

Finally, an entity may also be in the category "Hotel Facility". In this case, the unit is not assigned to a room type. Instead, it is a unit of the Hotel:

> "Concerning relaxation, you have the possibility to bring harmony between your body and your soul, thanks to the swimming pool, the Finnish sauna, the solarium, the fitness-room..."

While the fitness-room is quite obviously assigned to the hotel, it depends on the context to which entity the sauna is assigned. In this case, the sauna is related to the hotel.

> HotelToUnitRelation(HAC79/Sauna)

But as seen in this section the sauna can also be assigned to a room.

This domain has a sufficiently high complexity to motivate the architecture which is shown in the following section.

4.2. Applying the Method to the Hotel Domain

The project members were postgraduate students (M.Sc.) without prior NLP experience and without much knowledge about either machine learning or linguistics (Criterion C.1). The focus of the project was to find most of the relations while keeping the costs low. As shown in the previous section, a domain-specific dictionary is available with the OTA code list (D.1). The linguistic complexity of the project is also an important factor for choosing the appropriate architecture. In the given domain, typing and grammar errors are rare. Additionally, co-references could appear theoretically but could not be identified in the test corpus. Because most hotel descriptions are created by the hotel marketing departments, the sentences tend to be lengthy and sometimes have a high nesting depth. Overall, the linguistic complexity is considered relatively low (B.2).

Entity Mention Detection: Because the OTA code list was available as a mature domain dictionary, it was easy to create gazetteers (D.1). Including the gazetteers is also useful because the team had no prior NLP experience. This makes gazetteer lists a good starting point for EMD (C.1). The only customization effort related to the gazetteers was the consideration of synonyms. This was done manually based on sample data. The hotel domain is not linguistically complex. Therefore, it is not required to include a ML-based NER component (B.2).

Relation Mention Detection: The selection of the RMD approaches is also related to the considerations in EMD. No criteria would motivate a ML-based RMD system with the given project parameters.

According to the recommendations from the method, the application architecture chosen included rule-based RMD and EMD together with gazetteers.

4.3. Evaluation

An evaluation in terms of recognition accuracy was performed. The corpus contained a total of 227 hotel descriptions for 124 hotels. The corpus was split into two disjoint parts. One part containing 100 documents was used for optimizing the customization of the application, e.g., adding new synonyms to the gazetteer list and creating syntax patterns. In order to test the effect on new documents, the recognition rate accuracy was calculated using the second part of the corpus. For assessing the results, we use *Precision (P), Recall (R)* and *F-Measure (F)*, which are commonly applied measures from Information Retrieval. *P* describes the correctness, *R* describes the completeness and *F* is their weighted harmonic mean. Table 5 shows the results.

	F (EMD)	F (RMD)
Gazetteers based on OTA	0.75	0.72
Gazetteers based on OTA and synonyms	0.87	0.85

Table 4: Evaluation result

Generally, the results are satisfactory for the hotel domain. The data shows that the RMD recognition rate is mainly capped by the EMD recognition rate. By enhancing the gazetteers with synonyms of the OTA codes, the F-measure could be improved by 0.12 (EMD) and 0.13 (RMD), respectively.

The customization was implemented by four postgraduate computer science students (M.Sc.) without prior NLP experience in a six month timeframe. This indicates that the complexity of this domain could also be handled by a development organization in an industry project.

5. Conclusions

This paper presents a criteria-driven method for architecting domain-specific IE applications. We have developed evaluation criteria which balance various IE techniques in terms of costs and benefits. To our best knowledge, such a method that takes into account IE application development costs has not been presented before. We showed that this approach has been valuable for a real-world application scenario from the tourism domain. We argue that other domains could also benefit from it.

As future work, we plan to apply this method in more IE projects in order to review the validity of our statements. We assume that the tooling for ML-based RMD will emerge which would require a re-evaluation of the presented criteria.

6. Acknowledgement

This work was funded by HRS – Hotel Reservation Service.

7. References

Cunningham, H., Maynard, D., and Tablan., V. (2000) “JAPE: a Java Annotation Patterns Engine (Second Edition)”, Technical report CS-00-10, 2000, University of Sheffield - Department of Computer Science, Sheffield.

Finkel, J. R., Grenager, T., and Manning, Ch. (2005) “Incorporating non-local information into information extraction systems by gibbs sampling”, *Proceedings of the 43nd Annual Meeting of the Association*, 2005, Association for Computational Linguistics, Ann Arbor, Michigan, pp363-370.

Isabelle, P., Cunningham, H., Maynard, D., Bontcheva, K., and Tablan, V. (2001) “GATE”, Proceedings of the 40th Annual Meeting on Association for Computational Linguistics 2001,Association for Computational Linguistics, Stroudsburg, PA, USA, pp168-175.

Kozareva, Z. (2006) “Bootstrapping named entity recognition with automatically generated gazetteer lists”, Proceedings of the Eleventh Conference of the European Chapter of the Association for Computational Linguistics: Student Research Workshop, Association for Computational Linguistics , 2006 Stroudsburg, PA, USA, pp15-21.

Lafferty, J. (2006) “Conditional random fields: Probabilistic models for segmenting and labeling sequence data”, Proceedings of the 18th International Conf. on Machine Learning, 2001, Morgan Kaufmann, San Francisco, CA, pp282-289.

Li, Y., Bontcheva, K., and Cunningham, H. (2005) “SVM Based Learning System For Information Extraction”, Proceedings of Sheffield Machine Learning Workshop, LNCS, 2005, Springer Verlag, Heidelberg, pp319-339.

Marneffe, M., and Manning, Chr. D. (2008) “The Stanford typed dependencies representation”, Coling 2008: proceedings of the workshop on Cross-Framework and Cross-Domain Parser Evaluation, 2008, Association for Computational Linguistics, Stroudsburg, PA, USA, pp1-8

Miyao, Y., Sætre, R., Sagae, K., Matsuzaki, T. and Tsujii, J. (2008) “Task-oriented Evaluation of Syntactic Parsers and Their Representations”, Proceedings of the 46th Annual Meeting of the Association for Computational Linguistics, The Association for Computer Linguistics 2008, Columbus, Ohio, USA. pp46-54

OpenTravel Alliance (2010) OpenTravel Implementation Guide: Executive Summary, No. 1.5, 2010. http://www.opentravel.org/Resources/Uploads/PDF/OpenTravel_ImplementationGuide_v1.5_ExecSum.pdf, (Accessed 2 November 2011)

Surdeanu, M., Johansson, R., Meyers, A., Màrquez, L., and Nivre, J. (2008) “The CoNLL-2008 shared task on joint parsing of syntactic and semantic dependencies”, Proceedings of the Twelfth Conference on Computational Natural Language Learning. 2008. Association for Computational Linguistics. Stroudsburg, PA, USA, pp159-177

Surdeanu, M., McClosky, D., Smith, M. R., Gusev, A., and Manning, C. D. (2011) “Customizing an Information Extraction System to a New Domain”, Proceedings of the Workshop on Relational Models of Semantics, 2011, Association for Computational Linguistics. Stroudsburg, PA, USA.

Wyner, A., and Wim, P. (2011) “On Rule Extraction from Regulations”, Proceedings of the 24th International Conference on Legal Knowledge and Information Systems. IOS Press, Amsterdam, 2011.

Attacks to ZigBee and Wireless Sensor Networks Honeypots for Detection and Response

J. Markert[1], M. Massoth[2], K.-P. Fischer-Hellmann[2], S. M. Furnell[1]

[1]Plymouth University, Plymouth, United Kingdom

[2]Hochschule Darmstadt – University of Applied Sciences, Darmstadt, Germany

e-mail : jurgen.markert@plymouth.ac.uk

Abstract

ZigBee is a new communication technology and offers opportunities not only for developers, but also emerges as a possible risk containing flaws for an attacker to focus on. There is a trend in this field to develop methods for tracking intrusions and unauthorized access by an attacker, and for detecting attempted attacks against the stability of wireless sensor networks with intrusion detection systems. These systems represent the current state of the art in the field of research on detecting attacks on wireless sensor networks. We therefore propose implementing honeypots for ZigBee networks, which would be an alternative approach to intrusion detection systems, and which would prove to be ideal for the development of appropriate countermeasures. We feel that not enough research has been done so far in the development of ZigBee honeypots to offer opportunities for specific analysis and intercepting attacks.

Keywords

Wireless Sensor Network, ZigBee, Intrusion Detection System, Honeypot

1. Introduction

The next industrial revolution will be the internet of things, machine to machine communication, “smart homes”, “smart buildings” or even “smart cities” (Sorensen 2010). The concept is deceptively simple: Everything can be connected to anything else. Anything provides services and can be monitored and controlled. This evolution is already laid out and well on its way. IPv6 and other technical prerequisites are already available to cope with the challenge of having more and more systems to be addressed in a single network.

Yet, these networks don't necessarily have to be wire-bound. A lot of networking technologies have their focus on wireless communication channels. Many companies have worked together in the development of Bluetooth as a wireless standard. ZigBee was likewise introduced and developed to be an ideal standard for wireless sensor and control networks (ZigBee Alliance 2008). ZigBee is an additional feature set to the IEEE 802.15.4 standard and defines additional layers on top of it (IEEE 2006).

IEEE 802.15.4 defines physical radio and a MAC layer, providing a simple packet data protocol for lightweight wireless networks. ZigBee adds the layers for logical network, security and application software. ZigBee determines the API, and the ZigBee Alliance certifies ZigBee-compatible devices guaranteeing their interoperability (Elahi 2010).

New ways of interaction become available through ZigBee, offering great advantages and a lot of potential to save energy and make life much more comfortable, but also requires that underlying structures be robust, reliable, safe, and secure. The key aspects of network technologies are commonly the same: application developers are expected to protect communications in order to attain the classic information security requirements: confidentiality, integrity, and availability.

2. Motivation

The analysis of the security and reliability of ZigBee networks has shown that these aspects have not yet been resolved satisfactorily, depending on the chosen implementation. But not all of the above requirements are present in the various configurations. The background to this is as easy as might be: the intended purposes of wireless sensor networks vary widely. One of them is low power consumption, running independently for the longest possible time, another one is for these devices to be as interoperable, compatible and easy to use as possible. This is in direct conflict of nearly every security feature, because security needs computational power and thus results in a higher energy consumption. These

features also limit their ease of use and render interoperability problematic: Encryption details have to be distributed and managed, requiring a bigger feature set, more network traffic.

The paper by Fabbricatore et al. (2011) describes these problems in the area of smart homes. The authors see several problems for existing home automation solutions involving ZigBee. They propose using additional cryptographic extensions on top of ZigBee, or to change the protocol, should ZigBee remain insecure for their purposes.

3. Attack categories

Common attacks on wireless sensor networks (WSN) as described in current publications and literature are part of a range of working and well-known attacks on ZigBee networks: Eavesdropping, replay attack, sinkhole attack, selective forwarding, network flooding, firmware modification and code injection (DePetrillo 2009), (Goodspeed 2007), (Gu & Noorani 2008), (Masica 2007), (Wright 2009), (Yang et al. 2008). These attacks can be subdivided into three categories:

3.1. Resource drain attacks

The first category shall be termed “resource drain attacks”. These attacks target the power of network devices as shown in figure 1 (replay-attack). In a battery-driven system, the main goal of an attacker is to exploit the system's power consumption against the system itself. An attacker might render wireless sensor network unusable by making parts of it run out of battery power through the modification of networking schematics, with the propagation of new routes, and by incessantly sending and requesting data. Batteries are a limited resource, network capacity is likewise limited. An increasing network load limits cripples the already limited throughput of the network.

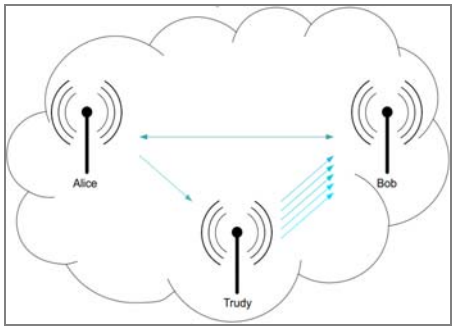

Figure 1: Power drain through replay attack

The authors Raj and Thilagavithy (2012) propose a solution to a specific type of network load caused by so called jamming attacks in wireless sensor networks. Due to the amount of commonly available radio channels in these networks, shifting to another network channel is suggested each time a jamming attack is detected. The authors claim that a residual network activity should keep the channel busy for a limited time during the short interval in which the jamming is not taking place as to make the jamming attacker believe that the jamming attack is successfully disturbing the WSN communication. This behaviour could also be described as deception, or, simply put, a honeypot or honeynet. This could even also attract an attacker and act as a decoy for the attacker.

3.2. Network attacks

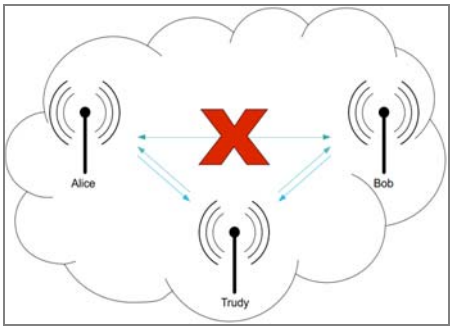

Figure 2: Network redirection for man in the middle scenario

The second category is called “network attacks”, describing the attacker's goal of modifying the network's routing structure. By this, the attacker aims to gain valuable information through redirection. He becomes therefore a “man in the middle” listening to any traffic.

3.3. Hardware-specific attacks

The third category is called “hardware-specific attacks”, standing for the goal to bring the networking nodes under complete control of the attacker (e.g. firmware modification as shown in fig. 3). This could be achieved with physical attacks like attaching wires in order to extract encryption keys from a network node. Attacks on hardware can also be an attack on firmware, resulting to firmware-modification. This is possible through security flaws in software-components of the nodes.

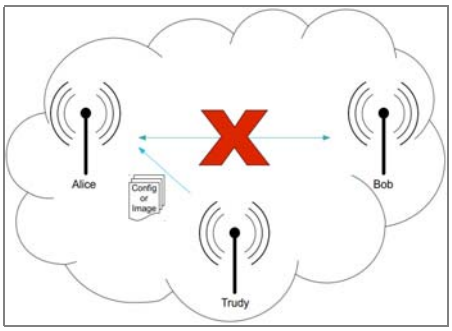

Figure 3: Firmware-modification attack

All of the three attack types mentioned above already exist. There is even a “proof of concept” worm that exploits network node communications and propagates itself over the network.

Goodspeed et al. (2012) have presented new results in the area of WSN hacking. They improved the killerbee API and wrote extensions to execute “wardriving” scenarios on ZigBee networks. They extended existing tools until all 16 ZigBEE channels could be monitored in parallel. They then combined this with a GPS signal logger for “wardriving” around the campus of Dartmouth. They also wrote semi-automatic tools to attack the networks with various different attack types. This development should make abundantly clear, that the security threats for ZigBee are real and serious and it is the conclusive proof that solutions to detect the attacks is are of crucial necessity.

4. Countermeasures by design

Several security features are implemented in ZigBee by design. “ZigBee PRO 2007” defines security mechanisms for authentication, encryption and trust centre functions (Elahi 2010).

Research on these features has however revealed some shortcomings. Security features might be circumvented or their imperfection could be used against the system. Successful attacks might last as long as the attacker wants. These can even not be analysed, because usually, there is no log of network activities and hence, attackers will leave no traces. There is no “packet capture” of attacks, and the probed exploit code is not available in the wake of an intrusion attempt. An attacker will not get noticed and therefore, will remain unidentified. It is hardly possible to gather the leftover information for forensic analysis.

There are clearly still problems in the process of improving the security features of ZigBee networks. Having blind faith and trust in the existing countermeasures is greatly unjustified. Radmand et al. (2010) showed in their comprehensive paper, that the cryptography used in ZigBee is not encompassing enough to cover all possible attacks. Some of the problems like confidentiality are solved encrypting the data stream. Yet, problems on the network layer such as replay attacks still remain. They also state, that the manufacturers should provide a minimum of security, due to problems with encryption keys stored in plain-text in the nodes. These could be extracted by an attacker tampering with physically captured ZigBee network nodes. There is hence a need for an intrusion detection system, and also for system reporting break in attempts.

5. Intrusion Detection System

Intrusion attempts are reported in classical network security solutions by so-called intrusion detection systems (IDS). They use only passive inspection to monitor all network activities for violation of regular use, and have no other function in the net. Intrusion detection systems rely on predefined policies describing normal network activity and normal behaviour. An intrusion detection system is generally a single point in the network, but it might additionally also be distributed on several hosts of the network.

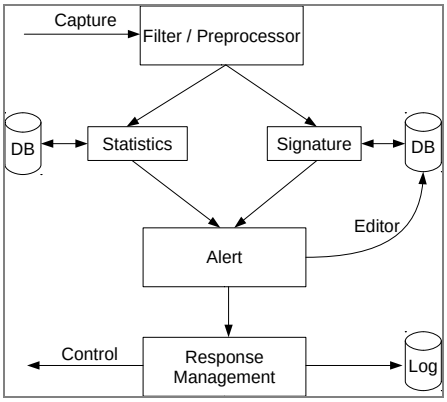

Figure 4: Intrusion detection system (IDS) working scheme

It might also stop intrusion or filter or modify malicious traffic as an active part of the network and is in this case most often called an intrusion prevention system (IPS). In an IPS, the controlling aspect of figure 4 is much more elaborate than in an IDS. All of these setups provide logging and reporting. In an IDS, every data packet has to be regarded and analysed. Its purpose is to spot the packets of an attack within a large amount of regular and normal network traffic. Processing every packet, its inspection, and the detection of attacks by matching patterns all require a lot of resources. In the context of ZigBee networks, and therefore battery driven network nodes with very limited resources, this is a clear drawback of an intrusion detection system approach in wireless sensor networks.

Kaplantzis et al. (2007) did a network simulation and had success in detecting selective forwarding attacks in wireless sensor networks by support vector machines (SVM), too. They also concluded that these attacks are the most difficult to accurately detect thus verifying assumptions made in previous research.

Sedjelmaci and Feham (2011) presented a novel IDS for the use in clustered WSNs. Using SVM, just like Kaplantzis et al. (2007) did, the essential point is to teach the detector nodes about normal network behaviour, such that they achieve a detection ratio of over 98% regarding abnormal network traffic.

Iwendi and Allen (2011) wrote a comprehensive paper on attacks on WSNs and demonstrated a way to simulate attacks with the intention of developing appropriate countermeasures. They propose in their conclusion the development of a security protocol for defensible WSN.

There is a definite need for security in wireless sensor network communications, and possible improvements should involve intrusion detection systems. The emerging outline can be briefly described as a sensor working on different network layers. It purpose is to detect anomalies in the net and to report these attacks. This is supposed to provide a new technical instrument for reacting to this new attack scheme. This feature set forms the common core of an intrusion detection and prevention system, also called a honeypot.

6. Honeypots

A honeypot can be described with a single phrase: It is a trap. It is in general an active system in a network monitoring every connection to this part of the network. The results are written to log files and reported accordingly. The honeypot looks like a normal node of the network to every system passing by. To an attacker, however, it will appear as a valuable target.

The advantages of a honeypot might be summarized as follows: instead of inspecting and analysing every packet of the network like an IDS, and then deciding whether this has been an attack or not a honeypot simply regards every connection as a likely attack. This behaviour saves a lot of resources because not every packet needs to be processed,

inspected and filtered for attacks. Even in the context of ZigBee networks and therefore battery driven networks, the honeypot system could make do with very limited resources. One of the drawbacks of a honeypot system approach in wireless sensor networks could be that it exposes additional targets which might get corrupted and then be taken over by an intruder. But since any other part of the net could equally get compromised, this is a small drawback. The advantages of a honeypot far outweigh its disadvantages.

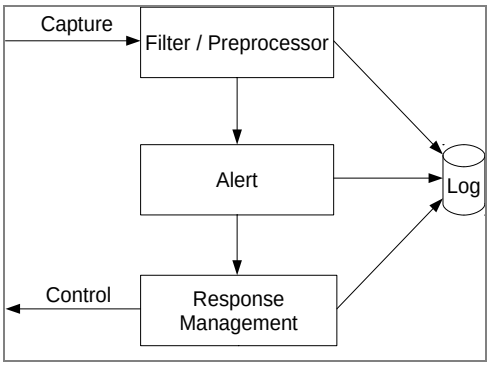

Figure 5: Honeypot working scheme

Prathapani et al. (2009) propose a honeypot system for the wireless mesh network standard 802.11s, then still in draft status. They set up the network simulator ns-2 and showed in their environment a very significant and successful result in network throughput with a high detection and low false positive ratio during a blackhole attack. Although these results were not proven to be correct in a real network, we assume that a similar result might be achieved in wireless sensor networks based on ZigBee standard communication.

Gupta et al. (2012) propose a honeypot technique for wireless mesh networks. A group of several honeypots are called a honeynet. The authors differentiate between different types of honeypots such as honeypots for research and honeypots for the productive environment. In detail they propose using a concept called honeyPHARM described by Hassan and Al Ali (2011). This solution has been specifically invented for the 802.11s draft. The authors Hassan and Al Ali (2011) propose a honeyPHARM, a distributed honeynet for the collection of malware in networks. Collected data will be used to discover new attack methods. This will be an addition to the nephentesPHARM system.

The authors Muraleedharan and Osadciw (2009) propose a framework using a honeypot technique combined with swarm intelligence for a battlefield monitoring application in a wireless sensor network. They state that traditional security schemes can not be applied in the field of WSN due to resource constraints. They had planned to build a simulation to prove this proposal, and validate the results.

The summary of all of these ideas leads to a proposed solution development of a honeypot for ZigBee networks without the drawbacks of a classical IDS. The concept of the honeypot will be presented below.

Several technical details are worthy of discussion. One of the proposed features of a honeypot should be that it might be temporarily part of the net at various different times. It should not always neighbor the same node in the network, because these nodes in the net might not be the target of the attacker.

One of the proposed features could also involve cloning. Those resources of special appeal to the intruder might duplicate themselves virtually during the course of an attack, expanding the target range and thus reducing the likelihood of an attack on the real network.

The system additionally features a feedback channel for reporting attacks. This can be probably done via a covert channel or other medium via a gateway. This might be done on other frequencies or channels like e.g. GSM, 5GHz WiFi, 868 MHz ZigBee, LAN and others.

A honeypot system should be a hardened system. Singh and Verma (2011) list a number of possibilities for hardening the WSN in the paper “Security For Wireless Sensor Network”. They also show the list of unresolved problems, and state that these problems are difficult to solve.

A honeypot must not be recognizable as such to an attacker. An attacked honeypot should therefore react in the same way as any other attacked part of the wireless sensor network. This leads to the assumption, that its hardware capabilities should be the same. For safety and reliability reasons, it could be equipped with a larger battery or a wired power supply.

In their paper, Mostara and Navarra (2008) suggest assigning roles in wireless sensor networks with specific features for honeypots. They propose progressively changing the roles of the honeypot nodes over the lifetime of the network. This feature should be part of the WSN honeypot as well.

Regular clients are forbidden from using the honeypots for networking purposes, since connections to these honeypots would be regarded as an attack. Since the roles of nodes in this network should change over time between honeypot nodes and regular nodes, a predefined schedule will be used to guarantee a low false positive intrusion detection rate. This method renders the network harder to attack.

Detecting new attack methods is definitely possible with honeypots. The rest of the network will be left in a functional state while the honeypots are under attack. As an additional benefit, new countermeasures can be prepared while the attack is still ongoing. All these presented uses of honeypots are suitable to increase the reliability and availability of ZigBee networks.

Moreover, the recording unknown attacks will undoubtedly lead to the development of new countermeasures and hardening. The proposed honeypot concept for ZigBee networks combines new detection mechanisms offering new countermeasures for the stability and reliability of the network.

The installation and maintenance of a single honeypot or of a distributed honeypot network clearly requires additional effort. Yet, this effort should be made on top of common improvements to the wireless sensor network like configuration hardening and regular firmware updates. Some implementations offering over-the-air programming features for updating nodes already exist.

The detection of an attack by a honeypot and the insight in the behaviour of an intruder can be used to devise appropriate defence mechanisms or to generate updates for the complete network. Considering the publications over the last year discussing new attack schemes, there is an expected growing market for researchers to do research on security flaws simply due to the also growing opportunities for intruders to mess with the ZigBee networks (Cache et al. 2010). Honeypots will help in detecting and resisting these unavoidably upcoming attacks. It should be understood, though, that the security of a ZigBee network is not static, but rather an ongoing process to be kept up during its whole lifetime.

7. Conclusions

ZigBee offers some security features out of the box. Its weaknesses, however, have been explored only in part to the present day. It appears that only few people have been doing research in this area at all, and no one has ever applied honeypot methods in a ZigBee network. Our intended research will explore previously unconsidered and unregarded aspects of security threats against ZigBee networks and develop new defence mechanisms with the use of honeypots.

8. References

Cache, J., Wright, J., Liu, V. (2010), “Hacking Exposed – Wireless”, MC Graw Hill.

DePetrillo, N. (2009), “Power Hungry People - Making Sense of New Critical Infrastructure Threats”, http://proidea.maszyna.pl/CONFidence09/2/CONFidence2009_nick_de_petrillo.pdf.

Elahi, A., Gschwender, A. (2010), “ZigBee Wireless Sensor and Control Network”, Prentice Hall.

Fabbricatore, C., Zucker, M., Ziganki, S. & Karduck, A. P. (2011), “Towards an Unified Architecture for Smart Home and Ambient Assisted Living Solutions”.

Goodspeed, T. (2007), “MSP430 buffer overflow exploit for wireless sensor nodes”, http://travisgoodspeed.blogspot.com

Goodspeed, T., Bratus, S., Melgares, R., Speers, R. & Smith, S. W. (2012), “Api-do: Tools for Exploring the Wireless Attack Surface in Smart Meters.”, 2012 45th Hawaii International Conference on System Sciences., IEEE, pp. 2133–2140.

Gu, Q., Noorani, R. (2008), “Towards self-propagate mal-packets in sensor networks”, WiSec '08: Proceedings of the first ACM conference on Wireless network security, ACM

Gupta, P., Rawat, P., Malik, S. & Gupta, S. (2012), “Securing WMN Using Honeypot Technique”, (4), 235–238.

Hassan, A. & Al Ali, M. (2011), “Collecting Malware From Distributed Honeypots - HoneyPHARM”.

IEEE, Institute of Electrical and Electronics Engineers - IEEE 802.15.4-2006 IEEE Standard (2006), http://standards.ieee.org/getieee802/802.15.html

Iwendi, C. O. & Allen, A. R. (2011), “CIA Security Management for Wireless Sensor Network Nodes”.

Kaplantzis, S., Shilton, A., Mani, N. & Sekercioglu, Y. A. (2007), “Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Support Vector Machines.”

Masica, K. (2007), “Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments”, http://csrp.inl.gov/Documents

Mostarda, L., Navarra, A. (2008), “Distributed Intrusion Detection Systems for Enhancing Security in Mobile Wireless Sensor Networks”, International Journal of Distributed Sensor Networks, Vol. 4, 2008.

Muraleedharan, R. & Osadciw, L. A. (2009), “An intrusion detection framework for Sensor Networks using Honeypot and Swarm Intelligence.”, Proceedings of the 6th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. IEEE.

Prathapani, A., Santhanam, L. & Agrawal, D. P. (2009) “Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks”.

Radmand, P., Domingo, M. & Singh, J. et al. (2010), “ZigBee/ZigBee PRO Security Assessment Based on Compromised Cryptographic Keys.”, 2010 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing., IEEE, pp. 465–470.

Raj, J. S. S. & Thilagavathy D. (2012), “Security Threats And Jamming Attacks Of Multi Channel Wireless Sensor Networks.”, International Journal of P2P Network Trends and Technology- Volume 2 Issue 1- 2012 (2), 27–31.

Sedjelmaci, H. & Feham, M. (2011), “Novel Hybrid Intrusion Detection System For Clustered Wireless Sensor Network.”, International Journal of Network Security & Its Applications 3 (4), 1–14.

Singh, S. & Verma, H. K. (2011), “Security For Wireless Sensor Network.”, International Journal of Network Security & Its Applications (3), 2393–2399.

Sorensen, S. (2010), “The Sustainable Network”, O'Reilly

Yang, Y., Zhu, S., Cao, G. (2008), “Improving sensor network immunity under worm attacks: A software diversity approach”, MobiHoc '08: Proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing.

Yüksel, E., Nielson, H. R., Nielson, F. (2010), “A Secure Key Establishment Protocol for ZigBeeWireless Sensor Networks”, Oxford University Press.

ZigBee Alliance (2008), “Latest ZigBee Specification Including the Pro Feature Set”, http://zigbee.org/Products/DownloadZigBeeTechnicalDocuments.aspx, Std. 053 474r17

Development of Three-Dimensional User Interfaces based on Low-Cost Inertial Navigation Systems

M. Muenter[1], M. Haid[1], T. Chobtrong, E. Guenes[1], M. Kamil[1]

[1] Competence Center for Applied Sensor Systems (ccass)
Hochschule Darmstadt – University of Applied Sciences, Darmstadt, Germany
e-mail: moritz.muenter@gmail.com

Abstract

The aim of this paper is to find a suitable technology that allows a three-dimensional position determination within a specific space using today's available sensor systems. Starting with a brainstorming, the key technologies inertial sensors, image processing and RFID were selected and elaborated in detailed concepts by methodological approach. Finally, the detailed concepts were validated on the basis of different application scenarios, as well as advantages and disadvantages discussed. The results revealed that the concept of an inertial navigation system has the most advantages in terms of feasibility, costs and computational effort. The camera system works precisely under ideal conditions but the system was not able to convince due to high processing power and issues of shadowing effects. The RFID concept offers potential for the future because the determination of position using RFID is a current subject of development. However, RFID was not able to prevail because of its low resolution and its liability to interferences. This paper sums up the key features of the inertial navigation system.

Keywords

INS, inertial navigation system, user interface, indoor navigation, object tracking

1. Introduction

In recent years, the interface between human and machine was only possible by means of external input devices in order to interactively work with a machine. Nowadays, screen and input peripherals are combined in a compact and mobile unit, the touch screen. Touch screens are a convenient tool for communication between human and machine. This enables the solution of two-dimensional communication tasks, such as the acquisition of objects whose main distinctive characteristics are located in the plane (e.g., hexagonal nuts, screws, circular). To recognize objects or to distinguish different levels of stacked objects, a touch screen requires the compulsory acquisition of the third dimension. A general three-dimensional object detection and representation therefore requires new technologies that are subject to this paper.

2. Inertial Navigation System

An Inertial Navigations System (INS) consists of accelerometers, gyroscopes, and magnetometers. For indoor navigation solutions these sensor types are mostly produced as micro-electro-mechanical systems (MEMS). The different sensor types of an INS are able to measure in all three space axis. With the recorded data of the accelerometer, the gyroscope, and the magnetometer it is possible to calculate the steric orientation and position. Short-term stability and the sensors bias require new filter models. To improve the accuracy of the measured orientation and position, Kalman-Filter can be helpful for estimating the position and orientation error (Haid *et al.*, 2004).

2.1. Hardware

For this project, an inertial measurement unit (IMU) was developed by the Competence Center for Applied Sensor Systems, which consists of two acceleration sensors, two gyroscopes, a magnetometer, a barometer, and a powerful ARM Cortex M3 processor as shown in figure 1. This board has been expanded with a Bluetooth interface that transmits measured data wirelessly to a PC. The board is operated by a lithium-polymer battery to operate independently. The processor performs the pre-processing of raw data coming from the sensors. The raw data is represented as digital units ("digits") and needs to be converted to SI-units for better visualization. Furthermore, the processor calculates the spatial orientation. For this purpose, the data of the accelerometers, the gyroscopes, and the magnetometer are merged using algorithms based on trigonometry. As a result, the spatial orientation in degrees for each sensor axis is transferred via Bluetooth.

Figure 1: Inertial Measurement Unit "CCASS IMU200" (Münter, 2011)

2.2. Software

The analysis and visualization of measured data is realized in MATLAB®. For this purpose, a graphical user interface (GUI), which is able to calculate spatial trajectories offline as well as online in real time, was developed. While moving the IMU, the IMU is visualized as a cube in a three-dimensional plot as shown in Figure 2. The cube changes periodically its actual position and its spatial orientation. For an off-line measurement, the data is stored in ASCII format. Using the ASCII formatted data the trajectory is calculated. This will facilitate the sharing of data between users. For online measurement, a virtual serial port is used. The measured data of the acceleration sensor and the angle of roll, pitch and yaw are comma-separately transferred.

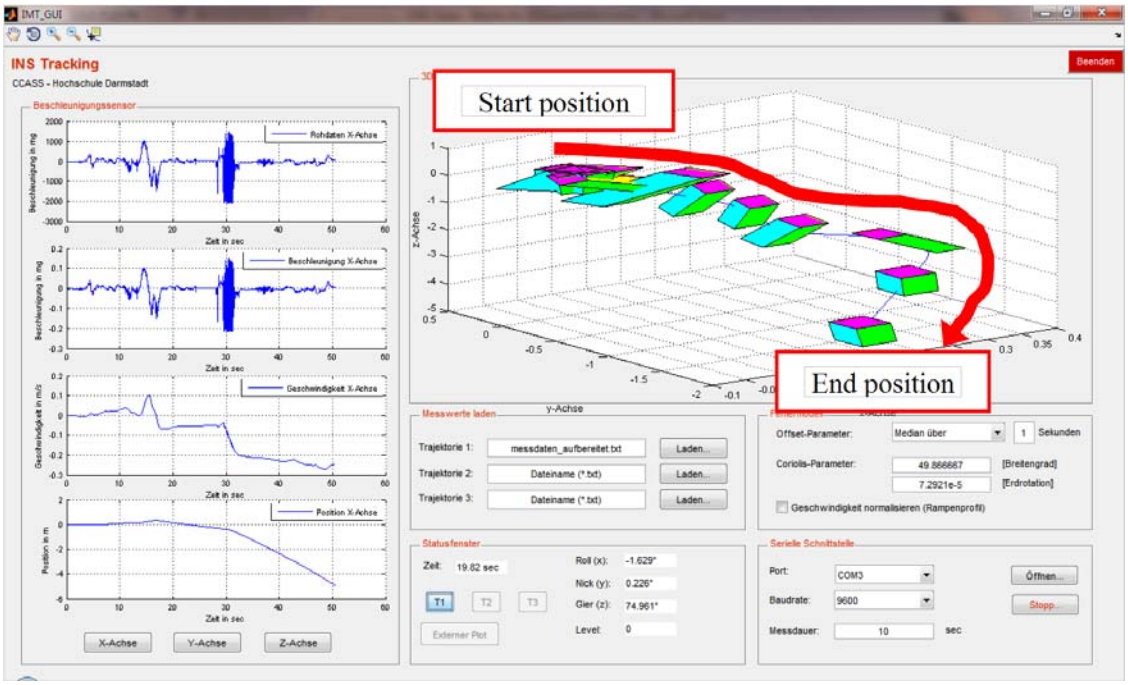

Figure 2: Graphical User Interface showing the trajectory of the IMU (Münter, 2011)

2.3. Algorithm

The MATLAB GUI receives the transmitted, comma-separated acceleration data and calculates the spatial position using double-integration and advanced filter algorithms. However, the accelerometer data contains errors. Thus, the gravitational acceleration is also recorded as static acceleration from the sensors, which can increase the square error in the position after a short time. To counteract, filters are necessary. Gravity has a direct impact on the acceleration sensors when the sensor axis is in the same direction vector of gravity. For this reason, the static offset, which is caused by the gravitational force, are compensated. The influence of gravity on each sensor axis is calculated by means of spatial orientation and acceleration data. That influence is subtracted from the acceleration data. The result is the

dynamic acceleration. Despite all, the dynamic acceleration still contains errors due to nonlinearity, linearity errors, and external influences such as temperature drift and accelerations caused by Coriolis forces. To compensate such influences and errors, a complex error model is required that takes part of all these factors and errors. Suitable filters are shaping filters and Kalman filter algorithms (Haid *et al*., 2004). Both shaping and Kalman filters calculate the optimal error based on an error model and derive the probable location. The use of such filters can also improve short-term stability of the acceleration sensors. Despite the computational complexity, real-time measurement is possible. The visualization, however, requires more computational effort, so the visualization is separated in the test trials for the calculation of the position (Münter, 2011).

3. Application scenarios

In the following, three innovative and creative application scenarios for a three-dimensional communication interface between human and machine are presented. In general, the idea is to create hands-on models with sensor technologies instead of creating virtual models. Hands-on models might be useful in customer relationship, particularly in dialogues with customers.

3.1. Interior Design

A possible application scenario is found in the interior design. When setting up a house or apartment CAD programs are usually used for interior furnishings. Using a computer, the designer creates a model fitting to the customers' requirements. The customer can influence the model only by direct communication to the designer. Instead, the interior of an apartment can also be designed interactively with the customer. For this purpose, it is assumed that the designer has objects such as chairs, plants, and desks as miniature models. These miniature models are equipped with an inertial sensor system as shown in figure 1. The miniature models are freely movable and can be stacked on a multi-touch screen for example. Each model has a virtual model that is stored on a computer. When raising a model with built-in IMU from one floor to the next level, a virtual model can be visualized in real-time. Craftsmen can use this virtual model later as a construction print. The big advantage for the customer in this scenario is found in the interaction with the miniature model, because the customer can be creatively active. This means a reduced workload for the designer, since the three-dimensional communication interface is ideal for rapid prototyping.

3.2. Entertainment Industry

In the entertainment industry innovative games are possible that can take place two-dimensional as well as three-dimensional. Otherwise, it would be possible to develop a three-dimensional Memory® game or intelligent domino cubes that recognize whether they are toppled over or not.

3.3. Emergency Management

Major incidents provide always a great challenge for authorities and organizations with security tasks such as the fire and rescue services. Unclear conditions and a large contingent of rescue teams require an extensive emergency management. A multi-touch screen would help the incident command to screen relevant information about dispatched vehicles and the affected object. Emergency vehicles and objects could be realized as miniature models, which are equipped with an inertial sensor system. By placing a model of a vehicle on the multi-touch screen, the vehicle is assigned to the emergency and could obtain current information from the incident command.

4. References

Haid, M.; Marquardt, G.; Melander, S.; Nguyen, P. (2004): Verbesserung der referenzlosen inertialen Objektverfolgung zur Indoor-Navigation durch Anwendung der Kalman-Filterung, Sonderdruck aus VDI-Berichte Nr. 1829, pp805-808

Münter, M. (2011): Konzeptstudie zur dreidimensionalen Objektverfolgung und Identifizierung, Hochschule Darmstadt, Competence Center for Applied Sensor Systems (CCASS), Darmstadt.

Chapter 2

Media

Demoscene Computer Artists and Community

C. Hastik, A. Steinmetz

Department of Media
Hochschule Darmstadt – University of Applied Sciences, Darmstadt, Germany
e-mail : canan.hastik@h-da.de

Abstract

The overwhelming variety of subjects in the field of born-digital content makes it difficult to classify and establish digital creative artwork. The lack of historical distance makes it even more difficult to identify art movements and summarize new art forms. Analyzing the Demoscene, a European subculture having the roots in the field of early computer generated graphic art, provides a first approach to structuring the scene and establish demoscene art as a facet of digital art. This formal structure is the basis for a conceptual solution in the field of digital preservation of complex dynamic media objects.

Keywords

Computer Demoscene, Digital Art, Ontology

1. Introduction

This contribution is part of a research to ensure the improvement of the long-term preservation of complex digital artefacts and the knowledge transfer of digital handcraft techniques. It is about analyzing and structuring the technology used materials and methods to constitute the Demoscene as an art movement.

The field of real-time audiovisual animation as one facet seems to be the royal discipline in which creative individual performances of various artistic handcraft practices are combined. This makes these computer-generated presentations, their platforms and not least the scene primary objects of research. A sustaining documentation of this vivid and largely undocumented world of sub cultural “Demo art” requires a fundamental understanding of the origins of tools being used which further allows the examination and analysis of artistic and experimental use of media technology.

Domain specific research, data collection and analysis take a key role in the context of documentation. Based on archives, portals and community websites relevant topics, objects and their relations have to be analyzed to visualize the context. An explicit analysis and characterization of the creative handcraft by the example of “Computer Demoscene” is mandatory.

2. The Computer Demoscene

Together with technical development niche cultures arise, forming their own norms, values and specific practices like net art, pixel art or Demo art. To distill the defining aspects of the Computer Demoscene, a historical overview is helpful.

The roots of the Demoscene reach far back to the first computer generated graphic art subcultures in the early 60s. Ben Laposky in the USA and Herbert W. Franke in Europe are considered as pioneers in the field of early computer art (Goodman 1987). Laposky’s creations of fleeting light images using a cathode-ray oscilloscope by supplying the deflecting electrodes with varying voltages based on different time functions is similar to classical elements used in Demo art. The same goes for Franke’s experiments programming geometric elements and curves on analogue and digital technology. This also applies to Charles Csuri’s first real-time animations and the usage of computer technology as a medium for art (Csuri 2012). His programmed functions with attributes manipulated by mathematical instructions are as sophisticated as algorithms used in Demo art.

The Computer Demoscene began in the early 80s where programming became a popular hobby activity. Until the 90s the scene was closely associated with the cracker scene. Demo artists initially developed small introductory presentations for cracked home computer games. This digital signature, so called Cracktro or Crack-Intro, was a start screen with logo of the cracker group, colored text, marquee with information on the game and greetings to friendly cracker groups, graphics, music and effects using the background color.

Figure 1: Crack-Intro (Fairlight, 1987)

Soon these cracktros became more spectacular than the games and developed into independent, real-time graphics, motion graphics and audiovisual arts.

2.1. Demoscene Insights

To complement their skills Demoscene artists formed groups of programmers, graphic designers and musicians, so called demo groups. The graphic artist wants to show how good he is at creating pictures and textures, the musician want to show how great he can compose and the programmer, also called coder, wants to demonstrate how well he can fit all together and what technical programming tricks and effects he can get out of the given hardware. The goal is to put the audience in awe, to impress and entertain.

The Computer Demoscene with their Demo art is a creative subculture with its own artistic expression and scene specific language. It is defined as “aspiring computer artists everywhere” (Shatz, P. 1993), “all people interested in demos” (Kuittinen 2001), “the scene, the demo community – a worldwide community of hobbyists interested in computer demos” (Reunanen 2010) and “a worldwide network of computer enthusiasts… a sub culture of the home computer culture” (Bolz 2011) producing “real-time, non-interactive applications along with music and graphics” (Scholz 2007).

These applications are executable programs that typically represent real-time audio-visual animations. Several special forms of Demo art products originated and were basically first classified by Borzyskowski in 2000 as follows:

Intro:	One or two routines
Dentro:	Preview of a demo
Demo:	More than two routines
Mega-Demo:	Linking of several demos.

A sampling survey of pouet.net, the largest web repository of news, groups and productions shows that Demoscene artworks today are primarily categorized into “Cracktros”, “Intros”, “Demos” and “Wild” (Pouet 2000). The category “Mega-demo” does not exist and just a few “Dentros” are collected. In total more than forty thousand artworks could be counted by crawling the portal and following the links to the original resources and collecting them.

Demo art type	Number of objects
Demo	ca. 24 000
Intro	ca. 5800
Cracktro	ca. 4400
4k	ca. 2000
64k	ca. 2000
Wild	ca. 1800
Invitation	ca. 1000
256b	ca. 700
1K	ca. 400
Dentro	ca. 350
Procedural graphics	ca. 150
Other	ca. 1700

Table 1: Different Demo art types and number of objects

It seems that the classification defined by Borzyskowski is not established or has changed due to technological change. One possible approach to the description of the basic structures of scene objects in form of an ontology is outlined in the following graphic. Objects, properties and their relations are exemplarily represented to visualize the context of Demoscene tools and materials today.

Over the years productions were subdivided into several competition oriented categories based on size limits and platforms they are designed for. Competitions are held on Demoscene events which are the most important community meetings for presenting new releases. For each event general competition rules and categories were defined. These rules and categories are indicative for an important quality criterion and are regarded as a constructive challenge within the scene. The general rules defining these restrictions seem to be not standardized and are changing gradually. On top of that some products cannot explicitly be assigned to only one category, they are categorized by size or not at all.

By analyzing the defined categories and rules of recent and older events published on the event websites, three main categories can be identified: Demo, Intro and others like graphics, music, wild, game and sub categories. While Demos are mostly categorized by hardware platforms like Commodore C64, Amiga, PC and Atari ST, Intros usually are classified by size limits like 4 kilobytes and 64 kilobyte and sometimes also by hardware platforms.

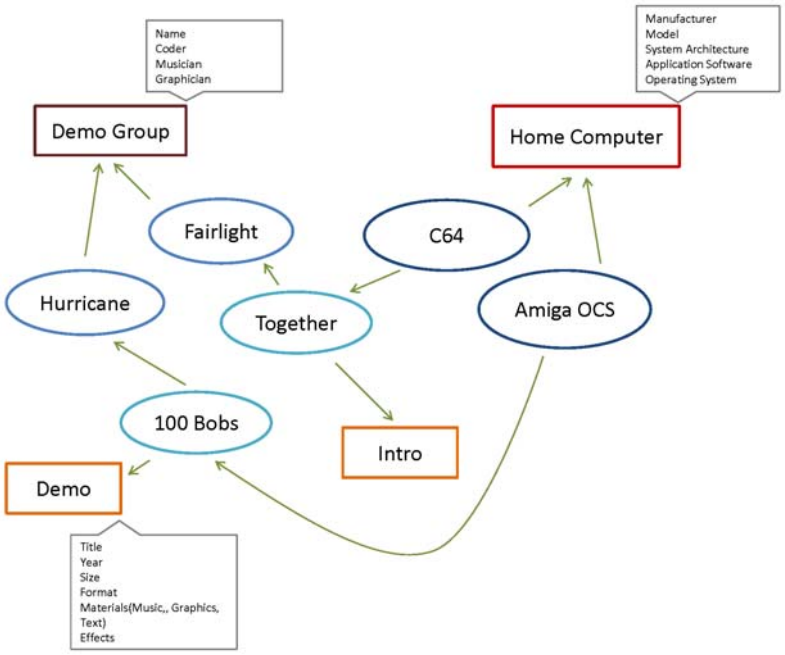

Figure 2: A model of Demoscene ontology

In total the use of over seventy different platforms can be counted, reaching from classic platforms like Commodore 64, Amiga and Atari ST to game consoles, handheld devices, mobile phones, operating systems and graphical user interfaces. Usually the activity is proportional to the actual distribution range of the platform, but also the access to appropriate development software plays a role.

2.2. Role of Hardware

First of all the “hackability” of the platform and its specifications formed the character of Demo artwork. Classic hardware with 8-bit, 16-bit and 32-bit architecture was commonly used.

Roughly speaking, with much effort not well documented or even inaccessible hardware was analyzed and reverse-engineered to create harmonically composed artwork with spectacular visual and audio tricks. Therefore a Demo programmer is often referred to as a craftsman who has mastered a particular cultural technique. The more simple the technological basis is, the more compact the net of aesthetic stimuli wants to be woven (Heikkilä, 2010) to realize always more complex and elaborate programmed tricks. It is expected that Demo artists will demonstrate their skills and pursue the principle to generate “... flashy bits written in custom assembly language and breaking every rules ..." (Shatz, 1993). In fact Assembler is still used for performance critical code but also programming languages like C++ are common. Beyond that there are various approaches of developing modular Demo editors. One example is mentioned at

this point, because it represents a reflection of the basic principles of the scene in dealing with resources and materials (farbrausch 2000).

From the impressive artistic artifacts that challenge the computer hardware at most, not only platform-specific styles but also compositional principles have emerged and are maintained until today (Hartmann, 2010).

3. Culture Techniques of Demo artists

The development of specific design techniques depends on the technical skills of the artist dealing with the machine, the tools and the scene specific handling of the existing repertoire of effects. Given hardware characteristics were successively studied and tested. However it can be observed that the use of new platforms will always build up on the use of an existing repertoire. On the one hand, active inventory, the backup and transfer of classical effects and principles of composition to new platforms is practiced. On the other hand, the new platform is used for more efficient implementation of established aesthetics and new versions of classic styles and principles arise.

3.1. Demoscene Classics

The structure of classic Demo art productions can be characterized by the use of classical elements which depends on the hardware. Graphics were animated with routines. Animations were made up of increasingly complex mathematically described objects and geometric shapes.

For platforms like C64 and Amiga OCS: text got scaled up and down, rotated, deformed, moved, fluttered and was typically presented in fast-paced or even dancing scroll effects or animation, tunnel, plasma, light and fire effects. Other classic old-school effects are for example the raster line interrupt and copper bar effect, both background effects that will display vertical and / or horizontal stripes of different resolution and color number on the screen. Programmers used clever tricks to make the elements look better and enriched them with as much effects as possible. Over time, highly complex effects and a variety of elements were used. While the classic Demo art also experienced a change in composition and content, Demos today are dominated by procedurally generated realistic 3D scenarios. With the widespread use of PCs in the mid 90s and the related variety of hardware a new era of the Computer Demoscene began. In contrast to the home computers, Demos on a PC may or may not work on another PC or are differently interpreting the program code. The Demo development was changing, screen composition, colors and innovative ideas came to the fore. Graphical presentation and fresh ideas had to convince the audience not only the technical masterpiece. Classic effects had to be reinvented or went out of fashion.

Faster processors and more computing resources were changing the possibilities previously limited by the hardware, for example playing a modest number of frames for a smooth, full-scale animation in the form of a film. The factor "real time" emerged as one most important quality criteria and principle of the Demoscene. Before real-time was the only way to animate images on the screen. For the viewer of a Demo it is not recognizable if a movie file or an executable program file with code-based animated graphics and sound is being played. He cannot monitor the real-time aspect. Real-time effects can only be judged based on the knowledge about the specific hardware requirements. If you record all Demos on video, it will not matter if one artist has released a Demo running ten seconds on ten floppy disks, or a Demo running 20 minutes on one floppy disk (Botz, 2011). By limiting the hardware and the size of the executable file not just comparability is achieved, but also the use of too many pre-computed animations is avoided (Reunanen 2010). These restrictions are regarded as a constructive challenge and are indicative for other important quality criteria of the scene.

3.2. Quantity and Tricks

Both the C64 and the Amiga only offer limited options to move objects horizontally and vertically on the screen. With this limitation a purely quantitative competition started.

Object to object records were broken, better written calculation routines became faster and more efficient. Same applies to image and sound productions. The available drawing programs for traditional platforms like for example Deluxe Paint for the Amiga generally provide all aspects of the graphics hardware. Users had access to a wide range of graphical features and effects limited to the original color graphics modes and the specifications of used hardware.

However, it was not uncommon improve them and make these add-ons available for free within the scene. Only through outstanding programming achievements and pioneering spirit existing limitations could be greatly exceeded and impressive graphics could be created. For example, special routines allow displaying up to 128 colors instead of the original 16 colors on a C64 screen (C64 Picture Gallery, 1999).

Figure 3: Hurricane – 100 Bobs, (Amiga-OCS-Demo, 1989)

4. Conclusion

The first analysis shows that the language used by the Demoscene community is formed by structural and social conditions but in fact the used language describes scene typical phenomenons. The variety of subjects and forms of Demo art based on a huge amount of platforms using certain tools makes it difficult to develop a classification of this art movement and distinguish established trends in the Demoscene.

This research exemplarily outlines artistic works and practices as well as digital production techniques of computer generated visual media art from the early 80s until today. The analyzed portal contains a lot of valuable resources and context information as well as community annotations, but many resources are no longer available and especially the use of metadata is not uniform or even standardized. These inconsistencies in the specification of data structures complicate the accessibility to Demoscene media assets for public.

In further research more data and facts have to be collected and methodically processed while taking determined criteria for preservation (Hastik 2012) into account. A survey of all available internet resources must be made to develop a standardized metadata model.

5. References

Borzyskowski, G. (2000), „The Hacker Demo Scene and it's Cultural Artifacts“, http://www.scheib.net/play/demos/what/borzyskowski/, (Accessed 15 March 2012).

Botz, D. (2011), *Kunst, Code und Maschine. Die Ästhetik der Computer-Demoszene*, Transcript Verlag, Bielefeld, ISBN:978-3-8376-1749-8.

C64 Picture Gallery (1999), „A Brief Description Of Graphic Modes”, http://www.studiostyle.sk/dmagic/gallery/gfxmodes.htm, (Accessed 21 January 2012).

Farbrausch (2000), “Fr-08: .the .product “, http://www.theproduct.de, (Accessed 15 January 2012).

Franke, H. W. (1957), *Kunst und Konstruktion. Physik und Mathematik als fotografisches Experiment*, Bruckmann, München.

Goodman, D. (1987), *Digital Visions: Computer and Art*. Abrams, New York. ISBN: 978-0810923614.

Hartmann, D. (2010), „Computer Demos and the Demoscene: Artistic Subcultural Innovation in Real-Time“, in Funke, J. et al. (Ed.): *Proceedings of the 16th International Symposium of Electronic Art*, Revolver Publishing, Berlin, ISBN: 978-3-86895-103-5.

Hastik, C. (2012), „Computer Technology- A Tool in the hand of the artist?“, in *Proceedings of Euromedia 2012*, Bukarest, Romania. (Accepted 02 March 2012)

Heikkilä, V.-M. (2010), „Defining Computationally Minimal Art (Or taking the „8“ out of „8-bit“), http://www.pelulamu.net/countercomplex/computationally-minimal art, (Accessed 15 January 2012)

Institut für Mathematik und Informatik (2012), “Der Computer als Werkzeug der praktischen Kunst und der Kunstwissenschaft”, http://stubber.math-inf.uni-greifswald.de/mathematik+kunst/computer.html, (Accessed 15 January 2012)

Klütsch, C. (2007), *Computergrafik: ästhetische Experimente zwischen zwei Kulturen. Die Anfänge der Computerkunst in den 1960er Jahren*, Springer, London, ISBN: 978-3-211-39409-0.

Kuittinen, P. (2001), “Computer Demos – The story so far”, http://mlab.uiah.fi/ ~eye/demos/#glossary, (Accessed 15 March 2012)

Pouet (2000), “Your online demoscene ressource”, http://www.pouet.net/ (Accessed 15 March 2012)

Reunanen, M. (2010), *Computer Demos – What Makes Them Tick?*, Licentiate Thesis, Aalto Univ., Helsinki.

Serexhe, B. (2011), *Substanz und Ethik in der Konservierung digitaler Medienkunst*, ICOM Deutschland. Mitteilungen 2011, Vol. 18, No.33, pp8-10.

Serexhe, B. (2012), *Digitale Herausforderungen, Digital Art Works: The Challanges of Conservation*, pp4-8.

Scholz, A. (2007), *Iconoclash: Opium for the masses*, in SCEEN magazine, no. 2, pp. 51-56.

Shatz, P. (1993) *Walkthroughs and Flybys*, Waite Group Press, Corte Madera, ISBN: 1-878739-40-9.

Cognitive prototypes and narrative thinking

P. Green

School of Art and Media
Plymouth University, Plymouth, United Kingdom
e-mail: paul.green@plymouth.ac.uk

Abstract

The emergence of interest in 'experience' over 'use' in interaction design has recast the role of the user from a 'cog in rational machine' to one who experiences technology as part of a living environment (McCarthy and Wright, 2004). This shift in emphasis is part of a longer discourse in HCI which charts a trajectory from expert user to social actor (Grudin, 1990; Bannon, 1991). As part of this shift from *usability* towards *experience* there has been an increasingly visible presence of an artistic attitude in a field of HCI. While the broader context of this research is concerned with the design of experience around responsive artefacts this paper concentrates on how 'narrative thinking' operates within the context of open-ended visual content. It promotes the decoupling of narrative from material artefacts and emphasises reader centric perspectives which hinge on personal experience and meaning making. The paper represents one step in an argument for establishing a narrative framework for creative practice with a particular interest in responsive artefacts.

Keywords

Narrative, visual content, cognitive narratology, theory

1. Introduction

While narrative has been the focus of some considerable attention in the arts, emphasis has largely been placed on media seen as best affording the sequential unfolding of a story. Those that have attracted commentary in relation to narrative have typically been media that implicitly support sequences of visual imagery such as comic strips, film, and animation. The current overlap between narrative and interaction is probably most evident in the field of game studies and the Interactive Digital Storytelling (IDS) community which fused the interests of Technologies for Interactive Digital Storytelling (TIDSE) and International Conference on Virtual Storytelling (ICVS) conference series. With the emergence of digital media practices there has been more explicit openness towards a concept of narrative which is user/reader centric and many strands of narrative discourse have emerged around topics such as intelligent agents, tools for authoring, user/player agency and the blending of concepts of agency and authorship. There has also been a significant increase in applications focussed on the benefits of interactive narrative for learning demonstrated through, for example, the work of the Kaleidoscope network. By and large these approaches focus on interactive artefacts as containers of stories with some exceptions which include mobile or situated storytelling evidenced through projects such as 'Murmur' initiated in 2003 or 'Remember Me' (Speed et al., 2010). The last example explores approaches implicating the artefact as a conduit for memories where objects tagged with QR codes offer concrete material evidence of events and experiences recounted by their owners. Here the artefact is a witness to events rather than a medium that actively narrates as a film or novel might do. Narrative can therefore be treated as offset from the material object.

While the wider scope of the research involves unpacking narrative experience in a social spatial context of responsive or interactive objects. This paper is a step towards that and focuses on decoupling narrative from artefacts. To this end it explores how a cognitive approach is one significant element that helps support a broader concept of narrative as a framework for creative practice.

2. Context

There are two observations with regard to recent approaches to narrative that help to provide some focus here about how it is possible to understand how 'narrative thinking' operates with respect to visual content. These observations come from outside of the discipline of visual art and relate to research in literary fiction and the social sciences.

First, within contemporary discourse involving narrative across media the selection of material for analysis seems often based on its suitability to extend existing concepts and metaphors into the discussion of new media technologies. Aaron Aarseth in particular has illustrated the way ill defined labyrinthine metaphors have been uncritically projected onto new technologies (1997, p. 7). In art and aesthetics discourse the emphasis on structural, or 'grammatical', features relating to *the plot*, derived in part from Saussurean linguistics, has affected a heavy constraint on identifying suitable media for analysis. This is despite ideas that emerged almost immediately on the heels of Francophone structuralism in

the 1960s and emphasised reader/audience centred constructivist perspectives on narrative. In literature for example interlinguistic and intertextual concepts in the work of M.H. Bakhtin and Julia Kristeva, as well as reader centred ideas from Roman Ingarden and Wolfgang Iser, in particular gave credence to the constructive role the reader played in actualising stories that were 'virtually' available in a text. In addition, those working more recently in the field of *cognitive narratology* recognise how certain strands of research within cognitive psychology can offer support to how we understand narrative in literary form. Such moves towards marshalling cognitive theories in support of understanding techniques employed in literary works also offer themselves favourably to an understanding of narrative in interactive and visual media.

A second observation is related to how the *narrative turn* in the social sciences has accumulated momentum in the last two decades. The attention to personal *small* stories relative to *canonical narratives* in this field implies a different concern with what narrative can offer as a method for generating knowledge or understanding. Within areas such as discourse and identity studies, for example, there is a particular concern with how narrative can support enquiries about cultural difference or the construction of personal identities. More generally contemporary narrative research in the social sciences often focuses on how we go about attributing meaning and significance to events in our daily lives. While arguably such research has its roots in a sociolinguistic strand of narrative research which emerged synchronously with the classic structuralist narratology, it has wielded far less influence over practitioners working in the visual arts. The attribution of meaning and significance to aspects of lived experience, which is a core feature of narrative theory in social studies, would appear to hold much benefit for contemporary media artists.

The following sections of the paper outline two important approaches in cognitive narratology before going on to discuss a particular case for visual media. The narrative turn in social practice mentioned above is not separately addressed but is instead inflected in the cognitive approaches outlined.

3. A case for cognitive narratology

3.1. Binary and scalar approaches to narrative

To help elucidate the case for applying a cognitive approach to narrative in visual media it is useful to illustrate a common methodological division where one view focuses on a *binary* or *situated* definitions of narrative while another takes narrative within a *scalar* model which allows for the transferability of stories across a variety of media. The first might hold to a position that versions of stories when moved through history or across media cannot be considered the same stories as their value and meaning is located in the situation and context of their telling (Smith, 1980, Aaron, 2009). One might also face contentions about the narrative status of photographs or paintings based on a premise that a minimum of two events must be cited as a necessary condition for narrative (Carroll, 2001, p. 119).The latter view looks for the ways in which essential narrative properties are variably manifested in different media and is the basic "hypothesis of classic structuralist narratology" (Herman, 2002, 2004 p. 51). Here a novel might be regarded as possessing more narrativity than a painting since it can demonstrate more of the essential properties of narrative (Ryan, 2006, p7-9). One might also find arguments for how certain media can enable narratable content - for example, the inner thoughts of a character cannot be explicitly represented in a painting but can in cinematic production with an omniscient narrator.

From the perspective of visual media the problem with the first view is that it does not account for what might generally to be thought of as narrative features in the image in Figure 1a. If narrative requires the depiction of two events this image does not appear to meet the basic criteria and fails to qualify as a narrative. Nevertheless it is hard to deny there is some quality of narrative that appears to be present in the image. In order to argue the case for narrative here it is then necessary to begin identifying what qualifies as an event and whether events need to be directly depicted in the frame of the image. While such analytic debates do occur in the literature, particularly around art and aesthetics – see Bence Nanay (2009) - the focus of the arguments often become political ones that defend the status of visual media. To shift focus away from the medium and instead emphasise the relationship or effect of the text on the viewer, reader, or audience, and the role the recipient(s) takes up in relation to participating in the construction of the content underlines contemporary approaches that are captured within the field of cognitive narratology.

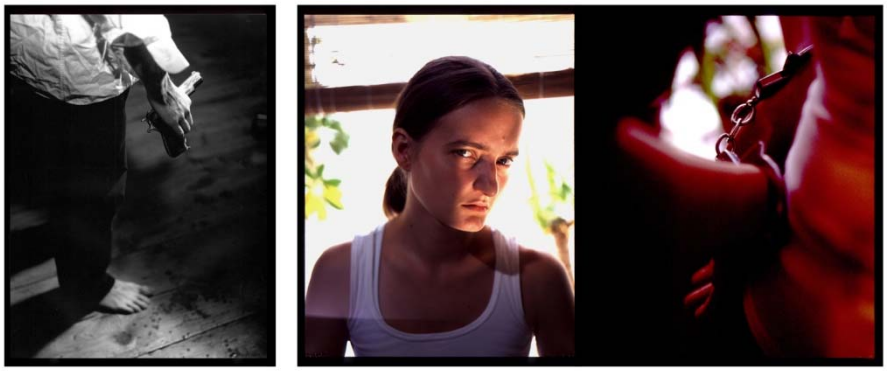

Figure 1

3.2. Preference rules and 'natural' narrative

Researchers working in this tradition come from various disciplinary backgrounds including cognitive psychology, social psychology, cognitive linguistics, discourse & conversation analysis, and contemporary literary theory. Of particular importance is the work of David Herman and Monika Fludernik. Herman has addressed concepts from cognitive science within the context of modern and contemporary cultural studies and literary art (2002, 2003, 2004, 2010), and Fludernik's efforts towards a 'natural narratology' (1996) are especially relevant in laying some of the ground for how cognitive approaches can be usefully applied in the context of visual and interactive media.

Herman is a leading figure in drawing together the argument for the application of cognitive science approaches to literary art. He shows how the field can be divided into major strategies that on the one hand focus on *making sense of stories* and on another underline *a sense making strategy*. While considerable crossover occurs between the interests of those researching in each of these strands one can summarise by saying the first deals with the way recipients of stories mentally articulate what is going on by interpreting specific cues in a text and the latter shows how stories can be used as tools for making sense of the world. The second strategy takes form in areas such as cognitive therapy, psychoanalysis, social and cultural studies of race and gender. The argument here for narrative in new media relates to how visual and interactive media can be processed in narrative terms and does not constitute an effort to create a new expanded definition of narrative which can suitably cater for visual and interactive media. Rather it makes a move towards exploring how narrative might be utilised as a method in creative practice by drawing on contemporary cognitive approaches that contribute to, what Herman calls, a 'second cognitive revolution' (2010, p.156). He defines a first cognitive revolution as a reaction to Behaviorism where the mind was viewed as 'software' running on the 'hardware' of the brain. This first revolution was constituted mainly by research in cognitive psychology and early artificial intelligence. The second revolution is concerned with a view of the mind which can be understood as intertextual, situated, relative, distributed, intermental, and social and takes in a much broader scope of disciplines that span science, art, and the humanities.

While Herman champions the second cognitive revolution he does not lose sight of the importance of classic structuralism. In Story Logic (2002) he outlines a preference based typology for action in narrative, reproduced in Figure 2, and discusses this in relation to different genres. This exemplifies the scalar approach, mentioned above in section 3.1, and helps to illustrate how established genres provide expectations about what constitutes action and how action is likely to be distributed in narratives of a given genre.

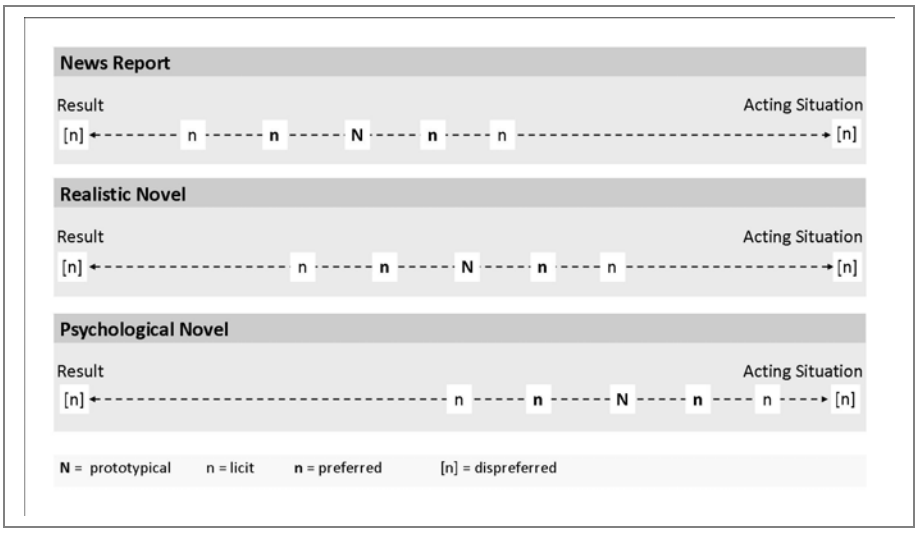

Figure 2: Typology of preference rankings for action representations in narrative as presented by Herman (2002, p.60)

The diagram represents three narrative genres with the preferred distribution of action prototypically placed between two poles – one pole focussed on *result* and the other on the *acting situation*. In this case 'result' indicates a tendency towards wrapping action in clear causal logic. The *acting situation* on the other hand is a term attributed to Georg Henrik Von Wright where a complete description of actions requires: 'a' an initial state before the action is initiated; 'b' an end state after the action is complete; and 'c' the state of the world had the action not occurred. This acting situation (which is the *possibility* for action between 'a' and 'b') weighs on the ability to compare the world as it is to some other counterfactual state that might have existed otherwise. The acting situation therefore can be understood as all the possibilities in between 'a' and 'b' that could rationally explain the event(s) that are explicitly available in a text – or image. The tendency towards open endedness in certain genres, such as the murder mystery or psychological novel, supports the aesthetic affordances of the genre which involves allowing the reader in to participate in constructing what it is that's going on. Frank Kermode's 'A Sense of an Ending' captures this participative activity of the audience in always looking forward from the current situation described in a story and attempting to narrow the possibilities for how it might end. In essence Herman shows there is no universal formula per se for how action should be depicted in all narratives whether we survey it synchronically across genres, as is the cases in Figure 2, or take a diachronic approach over generations of literature, as Fludernik did in her influential "Towards a 'Natural' Narratology" (1996). This text has served as a significant support to the emergence of the current thinking around cognitive narratology in relation to literary theory.

Like Herman, Fludernik does not see the cognitive turn in narratology as supplanting the ideas that arrived in the 1960s through Francophone Structuralism. Instead she sees a cognitive framework as being sufficiently expansive to account for postmodern narrative works that sat on the experimental or end of the spectrum. (2003, p. 264). The cognitive groundwork for her concept of a 'natural' narratology, which is useful to consider within the context of visual and interactive media, draws on three different sources of the term 'natural'. First is from a sociolinguistic tradition inspired by the groundbreaking work of William Labov and Joshua Waletzky (Labov, 1972) where natural narrative is associated with oral accounts of life experiences. Labov and Waletzky's method paired with Garfinkel's ethnomethodology (1967) significantly impacted on the development of conversation and discourse analysis and has been one of the major influences of contemporary interest in study of personal narrative. A second influence on Fludernik is in the area of cognitive linguistics that overlaps with prototype theory. Here a cognitive model of a bird is more likely to be represented as a crow or a sparrow as opposed to ostrich. Prototypical objects hence appear more 'natural' compared to other objects in the same category that are ranked less typical. Here Fludernik translates this cognitive notion of 'naturalness' to narrative by defining narratives of everyday experience - understood through exposure to contemporary fiction, news reports, or oral stories in conversation – as the prototype rather than those, for example, from previous generations or other centuries. Thirdly Fludernik was influenced by Jonathan Cullers notion of naturalness located in how readers blend or synthesise inconsistent information presented to them in a text. For example, rather than rejecting contradictory character behaviour or narration as implausible, a reading or viewing audience more often show a willingness to normalise the character's behaviour by filling in gaps in logic or action. Fludernik uses Ishiguro's butler Stevens in 'Remains of the Day' to illustrate this concept and points to the 'unreliable narrator' as an instance of this type of reading strategy (Fludernik, 2003, p. 251). In both of the approaches underlined by Herman and Fludernik above factors outside of the text contribute to how information explicitly presented in the work gets remoulded by an active reader.

3.3. Narrative gapping and significance

Narrative as a mode of human communication has been recognised as demarcating and reflecting *significance* in human experience. A key constituent of William Labov's theory, for example, is *evaluation* which is identifiable as a linguistic structure in talk and functions to orient the listener in a conversation towards the *point* of the story - why it is worth telling, or why it was a significant experience from the perspective of the narrator (Labov, 1972, p.366-75). As far as prototype theory goes the significant image (e.g. crow) of a given category (e.g. birds) referenced in a story is the particular cognitive image that surfaces in a readers/viewers/listeners consciousness. In narrative we can also recognise a nexus of prototypes in any given scene. For example, in a stereotypical bar fight which descends into chaos and involves characters breaking furniture over each other, we are unlikely to have an initial image of the item of furniture being IKEA bookshelves. Based on prototypes of bar fights we might be familiar with, such as in Westerns, an inventory of weapons will include bottles and glasses half full, and furniture will usually be constrained to chairs and possibly small bar tables. Any shock or humour we might experience from the representation of such a scene will often involve veering away from, while at the same time referencing, the prototypical inventory of weapons. Significant elements that support the construction of narrative therefore may be referenced but not necessarily made explicit in a text or image. Seymour Chatman's account for instance notes how *selection* is one of two principal features of narrative and is described as: "the capacity of any discourse to choose which events and objects to actually state and which only to imply" (Chatman, 1978, p. 28). While gapping is a necessary feature of communication in the narrative arts the gaps in action follow preference rules for different genres, as suggested by Herman, and are also naturalised, in Fludernik's sense.

Regarding independent still images, an untitled image in a gallery for example, the gaps are in fact what are salient. What it is that is not stated becomes the significant feature, the piece that the reader or viewer must themselves supply. Among a range of techniques noted in the study of narrative painting, for instance, the *punctum temporis* isolates a slice of action or moment in history which allows the viewer to unfold the possible events backwards and forwards from the moment in time depicted. Examples of neoclassical painting, such as that by Jacque Louis David, are often selected by aesthetic theorists to demonstrate the concept at work in still images (Nanay, 2009, Steiner, 2004). And while one could argue that such a salient visual moment does not 'tell' a specific story as a text might do, a cognitive narratological perspective can account for it by holding up what is 'natural' to a genre and how it offers up particular prototypes from which the viewer can extrapolate.

4. Case study

This case study attempts to ground some of the above concepts in a short discussion of two images which were exhibited together as a diptych (Figure 1b). In their original context the images were framed and hung side-by-side in a gallery. The two images might be said to be connected on a number of different levels. First of all they exist synchronously in front of a viewer and therefore are physically associated in spatial terms. One can also say they are stylistically or aesthetically associated in the sense they conform to one style of photography. They appear to be produced without any obvious postproduction and the lighting is similar in both. The images contain certain cues – related to the character clothing and posture as well as details in the environment - which would suggest the person depicted in both images is the same individual. If we can assume it is the same person in both images it is possible to proceed to further inferences about the time difference between the images and the role of the photographer. The handcuffs suggest not only some illegal action but also the prisoner is possibly in transit and therefore unlikely to be unaccompanied in this situation. Before moving to construct probable 'cause' about what has she may have done, it is clear that we have already made a number of assumptions since there is clearly no firm evidence that these images involve the same individual. It does seem reasonable, or at least possible, to continue on a deeper process of reasoning drawing on the emotional expression of the subject to infer a particularly troublesome attitude. Our judgement of the subject hinges on whether the expression is read as *confrontational in the face of authority* or *resilient in the face of injustice*. Either way the reading is bound to produce different paths of consideration that articulate the most prototypical explanation of what it is that is going on.

To avoid make the above assumptions about these images they were presented over three sessions to small groups of subjects totalling 28 participants. Without any prior notice they were given approximately 2 minutes to write about what it was they believed was going on in the images. No other information was provided such as a title or information about the original context of the images in the gallery setting; neither was any clue provided as to whether they were to be integrated into a publication, or for what reason the images were produced. The images were projected in a lab in full screen presentation mode shielded from the computer desktop environment. In each session the written statements were collected immediately afterwards and some questions were put to the group as to why a particular statement such as 'she is being arrested' could be justified. This discussion went on for approximately 5 minutes after the statements were collected. The majority of subjects indicated that 'she' was 'being arrested'. When asked how they could know this all noted the handcuffs. The shirt was explicitly singled out as evidence that the images represented the same individual

despite the large degree of colour distortion between the images caused by tungsten lighting at the time of the shoot. When asked how they could know that the handcuffed character was a female, one subject insisted it was the curvature of the torso while others indicated the connections to the character in the left panel made due to the shirt. When asked why she was being arrested one subject volunteered that it was something 'bad..a stabbing?' and this was partially qualified by the 'dirty look.. she gives you'. The reason given for such a specific association was that "..she looked like someone previously seen on the news.." who had conducted such an act. Another response to the question about the crime was that she was abroad and that it might be "..something to do with drugs." The rationale offered for the girl being abroad girl was that she was tanned, the blinds in the background looked like they were from a beach hut and the plants seemed exotic. In addition the association with a particular recent TV documentary series about people being incarcerated in foreign countries was directly referenced as influencing this interpretation.

The rationale provided by the participants illustrates the extent to which the concepts of 'prototyping' and 'natural narrative' account for the construction of fictive events not depicted in images. In practice it is possible for subjects to extrapolate out from an open ended sign such as a facial expression to a very specific proposition about an action that is in fact not depicted. While such as proposition might not be successfully defended in factual terms this has no bearing on what a viewing subject may experience or imagine to be happening since narrative logic does not depend on empirical causality. The limited information explicitly depicted in Figure 1b allows us to draw on life experience and knowledge about our own world to 'naturally' infer what it is that is going on. Marie-Laure Ryan, who has made significant moves in addressing narrative across media, including visual and interactive works, might explain this through the 'principle of minimal departure'. This refers to how, when we are exposed to a world represented in an artwork we invariable imagine it to be a mirror of our 'actual' world until some detail of the text or image contradicts our assumptions. Ryan holds that we insert our own descriptions of prototype worlds, entities, actions, events, and social behaviours until the evidence in the work breaks the prototype and forces us to engage with an alternative 'possible world'. This creative intervention in, or subversion of, the prototype is what makes a work engaging; without such interventions we are left with cliché. And while cliché is recognisable and in a design context supports 'usability', it is not necessarily useful for producing significant 'experiences' for viewers.

5. Conclusion

In this paper I have presented a case which favours decoupling narrative content from the material artefacts. I have attempted to demonstrate how a cognitive approach to narrative, illustrated primarily through the work of David Herman and Monika Fludernik, can be support such a view. By displacing the artefact as a centralised container of narrative and instead exploring how it makes use of cues that trigger narrative thinking in subjects it is possible to extend the study and discussion of narrative to situations that are generally excluded from narrative enquiry. This perspective is one level in a broader context of investigation which explores how narrative logic can be useful as a support to the design and development of spaces that incorporate static and responsive artworks. In this way, through making use of narrative methods currently being applied in other disciplines, we may get closer to understanding how creative practitioners use the prototypical social, or 'natural', world as a resource for constructing engaging and memorable experiences.

6. Acknowledgements

I wish to acknowledge Crawford College of Art and Design and the CIT Research Office for the award of a grant which has supported the wider research associated with this project.

7. References

Aaron, S. (2009), "Story Identity and Story Type", *The Journal of Aesthetics and Art Criticism,* 67**,** 5-13.

Aarseth, E. J. (1997), *Cybertext : perspectives on ergodic literature,* Baltimore, Md., Johns Hopkins University Press.

Bannon, L. (1991), "From Human Factors to Human Actors:The role of Psycology and human-computer interaction in system design", In J. Greenbaum and M. Kyng (eds.), *Design at Work: Cooperative Design of Computer Systems,* 25-44, Hillsdale. N.J.:Erlbaum.

Carroll, N. (2001), *Beyond aesthetics : philosophical essays,* Cambridge, UK ; New York, Cambridge University Press.

Chatman, S. B. (1978), *Story and discourse : narrative structure in fiction and film,* Ithaca, N.Y., Cornell University Press.

Fludernik, M. (1996), *Towards a 'natural' narratology,* London ; New York, Routledge.

Fludernik, M. (2003) "Natural narratology and cognitive parameters", *in:* Herman, D. (ed.) *Narrative theory and the cognitive sciences.* Stanford, Calif.: CSLI Publications.

Grudin, J. (1990), "The computer reaches out: the historical continuity of interface design", in *Proceedings of the Proceedings of the SIGCHI conference on Human factors in computing systems: Empowering people* (Seattle, Washington, United States, 1990). ACM.

Herman, D. (2002), *Story logic : problems and possibilities of narrative,* Lincoln, Neb, University of Nebraska Press.

Herman, D. (2003), *Narrative theory and the cognitive sciences,* Stanford, Calif., CSLI Publications.

Herman, D. (2004), "Towards a Transmedial Narratology" *in:* Ryan, M.-L. (ed.) *Narrative across media : the languages of storytelling*. Lincoln: University of Nebraska Press.

Herman, D. (2010), "Narrative theory after the second cognitive revolution" *in:* Zunshine, L. (ed.) *Introduction to cognitive cultural studies.* Baltimore: Johns Hopkins University Press.

Labov, W. (1972), *Language in the inner city; studies in the Black English vernacular,* Philadelphia,, University of Pennsylvania Press.

McCarthy, J. Wright, P. (2004), *Technology as Experience,* MIT Press.

Nanay, B. (2009), "Narrative Pictures", *The Journal of Aesthetics and Art Criticism,* 67**,** 119-129.

Ryan, M.-L. (2006), *Avatars of story,* Minneapolis, University of Minnesota Press.

Smith, B. H. (1980), "Narrative Versions, Narrative Theories", *Critical Inquiry,* 7**,** 213-236.

Speed, C. (2010), *Remember Me*. http://www.futureeverything.org/ festival2010/rememberme.

Steiner, W. (2004) "Narrative Pictures", *in:* Ryan, M.-L. (ed.) *Narrative across media : the languages of storytelling.* Lincoln: University of Nebraska Press.

Chapter 3

Business