Writing Cyber Security Term Papers

A Collection of Heuristics

Stephen D. Wolthusen
stephen.wolthusen@rhul.ac.uk

Department of Information Security and Communication Technology
Norwegian University of Science and Technology, Norway

and

Department of Information Security
Royal Holloway, University of London, United Kingdom

11 December 2023

Contents

Introduction

Referencing

Literature Sources

Plagiarism

Structure

Conclusions

How Hard Can It Be?

Key Data

Deadline for submission is **28 March 2024, 1400 hours GMT**

Please submit the paper as a single PDF file via Moodle *in the correct submission folder* for your module code

- Late submission folders will be set up, but these are **only** to be used for extensions registered and approved via the EPMS office — unauthorised late submissions will be automatically rejected

The target (and *soft* maximum) length of the paper is:

IY3612	2000 words
IY4612	3000 words
IY5612	4000 words

Introduction

The **term paper** is meant to be an essay typically taking the form of a *structured* literature review

No original work is sought (although this is not ruled out entirely), but similar to an original research paper, a literature review benefits from clear and concise **research question(s)**

- This will help select and filter articles, chapters, and conference contributions for their relevance to answering the question at hand — otherwise it is very easy to get sidetracked
- These question(s) should normally be made explicitly visible

Choice of Topic

You should choose your own topic satisfying the following constraints:

- Topics must be immediately relevant to Cyber Security, i.e. either directly related to material covered, or immediately adjacent to it
- Material covered should not overlap substantially with what is already presented in lecture materials
- A reasonably narrow focus is advisable — even if this is intended as a literature survey, technical depth and analysis is required, rather than merely a summary of results

Example Topics

An in-depth study of a reasonably recent attack campaign or reviewing 2–3 primary research articles on a topic related to the module’s areas would be good examples

Referencing and Citations

In any academic writing, good referencing is important

- Where arguments are being reproduced, or results summarised, accompany this with a reference, even if the same source has been cited previously: Citing a source once and relying on it in several places is not adequate
- Citation styles vary, but should be sufficient to easily find the source
- You can use LaTeX (with BibTeX or Biber), Endnote etc. — use of a citation manager is advisable if only as a dry run for larger pieces of work later (Overleaf works, but has licence restrictions)
- Recommendation is to use the ACM citation style [O'Brien et al., 2008]; this defines formatting for a number of different publication types (and when using BibTeX, this is formatted automatically)

ACM Citation Example

O'BRIEN, H.L. AND TOMS, E.G. 2008. What is user engagement? A conceptual framework for defining user engagement with technology. Journal of the American Society for Information Science and Technology, 59, 6, 938-955.

Sources of Literature

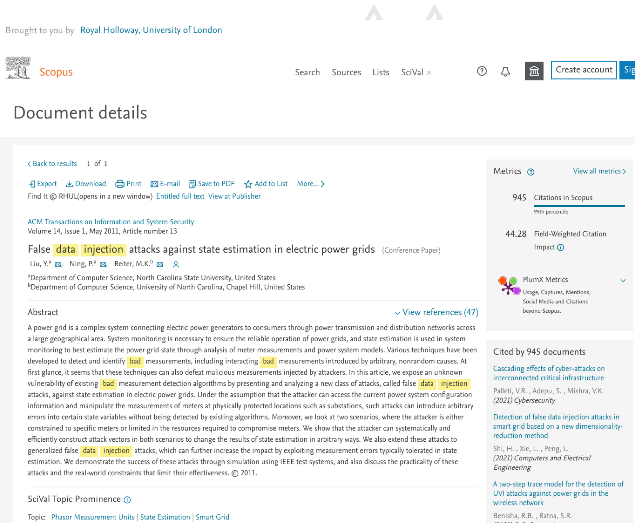
Meta-Collections

Meta-Collections are not deposits of reference as in the case of publishers,

- **Scopus** Partially hand-curated database including material from other (paywalled) publishers. Allows forward and backward tracing of citations
- **DBLP** Curated database of journals and conferences in most areas related to computer science, usually very clean meta-data. Free to access, but links to sources require permission (usually via college/UoL subscriptions)
- **Google Scholar** Collects papers found outside paywalls by crawling, contains plenty of duplicates and citation counts are unreliable at best.

Sources of Literature

Examples (1) — Scopus search



Brought to you by Royal Holloway, University of London

Document details

< Back to results | 1 of 1

Find It @ RHUL(opens in a new window) Entitled full text View at Publisher

ACM Transactions on Information and System Security
Volume 14, Issue 1, May 2011, Article number 13

False data injection attacks against state estimation in electric power grids (Conference Paper)

Liu, Y.[a], Ning, P.[a], Reiter, M.K.[b]

[a]Department of Computer Science, North Carolina State University, United States
[b]Department of Computer Science, University of North Carolina, Chapel Hill, United States

Abstract

View references (47)

A power grid is a complex system connecting electric power generators to consumers through power transmission and distribution networks across a large geographical area. System monitoring is necessary to ensure the reliable operation of power grids, and state estimation is used in system monitoring to best estimate the power grid state through analysis of meter measurements and power system models. Various techniques have been developed to detect and identify bad measurements, including interacting bad measurements introduced by arbitrary, nonrandom causes. At first glance, it seems that these techniques can also defeat malicious measurements injected by attackers. In this article, we expose an unknown vulnerability of existing bad measurement detection algorithms by presenting and analyzing a new class of attacks, called false data injection attacks, against state estimation in electric power grids. Under the assumption that the attacker can access the current power system configuration information and manipulate the measurements of meters at physically protected locations such as substations, such attacks can introduce arbitrary errors into certain state variables without being detected by existing algorithms. Moreover, we look at two scenarios, where the attacker is either constrained to specific meters or limited in the resources required to compromise meters. We show that the attacker can systematically and efficiently construct attack vectors in both scenarios to change the results of state estimation in arbitrary ways. We also extend these attacks to generalized false data injection attacks, which can further increase the impact by exploiting measurement errors typically tolerated in state estimation. We demonstrate the success of these attacks through simulation using IEEE test systems, and also discuss the practicality of these attacks and the real-world constraints that limit their effectiveness. © 2011.

SciVal Topic Prominence

Topic: Phasor Measurement Units | State Estimation | Smart Grid

Metrics

View all metrics >

945 Citations in Scopus
99th percentile

44.28 Field-Weighted Citation Impact

PlumX Metrics
Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

Cited by 945 documents

Cascading effects of cyber-attacks on interconnected critical infrastructure
Palleti, V.R. , Adepu, S. , Mishra, V.K.
(2021) Cybersecurity

Detection of false data injection attacks in smart grid based on a new dimensionality-reduction method
Shi, H. , Xie, L. , Peng, L.
(2021) Computers and Electrical Engineering

A two-step trace model for the detection of UVI attacks against power grids in the wireless network
Benisha, R.B. , Ratna, S.R.

Sources of Literature
Selected Publishers

Publishers requiring paywalled access (via college VPN or on campus):

SpringerLink Not all publications are accessible via RHUL/UoL subscriptions electronically, but e.g. most LNCS conference proceedings and many journals are

ScienceDirect Not all publications are accessible via RHUL/UoL (covers many disciplines)

IEEE Xplore Most material available, not all publications are at the same quality level

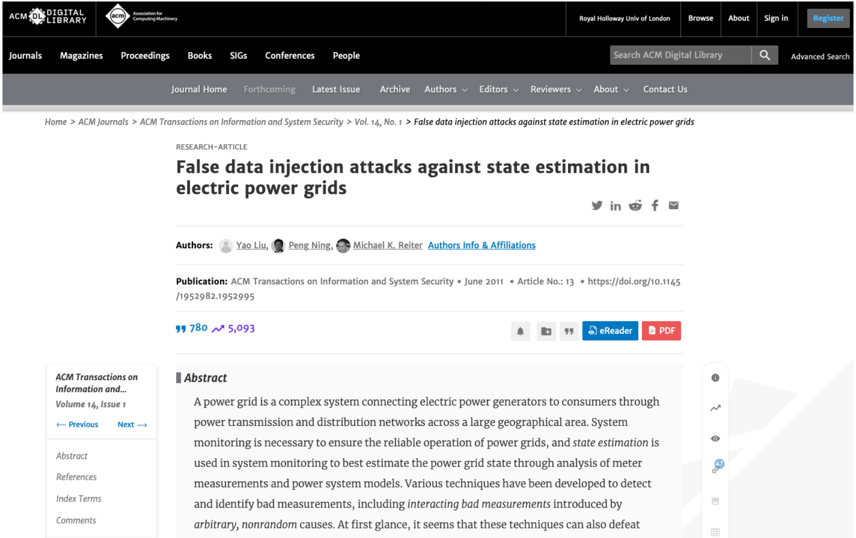
ACM Digital Library Complete archive of Computer Science publications back to 1958

arXiv Not a publisher as such, but will hold both pre-prints and some original work across mostly physics, mathematics, and computer science, no paywall

Cryptology ePrint Archive Preprint archive for cryptographic research, no paywall

Sources of Literature

Examples (2) — ACM DL Article View



Home > ACM Journals > ACM Transactions on Information and System Security > Vol. 14, No. 1 > False data injection attacks against state estimation in electric power grids

RESEARCH-ARTICLE

False data injection attacks against state estimation in electric power grids

Authors: Yao Liu, Peng Ning, Michael K. Reiter Authors Info & Affiliations

Publication: ACM Transactions on Information and System Security • June 2011 • Article No.: 13 • https://doi.org/10.1145/1952982.1952995

Abstract

A power grid is a complex system connecting electric power generators to consumers through power transmission and distribution networks across a large geographical area. System monitoring is necessary to ensure the reliable operation of power grids, and *state estimation* is used in system monitoring to best estimate the power grid state through analysis of meter measurements and power system models. Various techniques have been developed to detect and identify bad measurements, including *interacting bad measurements* introduced by *arbitrary, nonrandom* causes. At first glance, it seems that these techniques can also defeat

Defining (and avoiding) Plagiarism

Consider for example the IEEE Publications Board definition of plagiarism:

Plagiarism

> . . . the use of someone else’s prior ideas, processes, results, or words without explicitly acknowledging the original author and source

Copying results (duplication of text, even with minor alterations) without acceptable attribution

- Can be detected automatically in part, but still surprisingly prevalent

Plagiarism includes:

- Not quoting passages taken directly; appropriate references are required in addition
- Paraphrasing without proper references
- Use of arguments, data, or evidence from other authors without references

Other Academic Misconduct

Academic misconduct is not limited to plagiarism and also includes (but is not limited to)

- Collusion
- Contract cheating
- Use of unauthorised aids (specifically including generative models)

Candidates may be called upon to explain and justify their work, and current regulations do no longer between minor and major cases of academic misconduct

When in doubt refer to the academic regulations, specifically relating to academic misconduct

Structuring the Paper

A term paper is relatively short and hence will not have a very elaborate internal structure, but will be broadly along the following lines:

1. Introduction
2. Background (*optional*)
3. Problem Areas (*one or several, depending on questions*)
4. Discussion and Analysis
5. Conclusions
6. Appendices (*if any*)

followed by the list of references

Writing Introductions

Modified Stirewalt Approach for Introductions

Writing introductions is hard, but the following is a **heuristic** that may help in their formulation as four concise paragraphs:

Introduction What is the problem and why is it relevant to the audience? Needs to be concise

Background Elaborate on why the problem is hard, critically examining prior work, trying to tease out one or two central questions

Details How were the challenges addressed? Can be formulated as a form of syllogism, also addressing assessment and validation

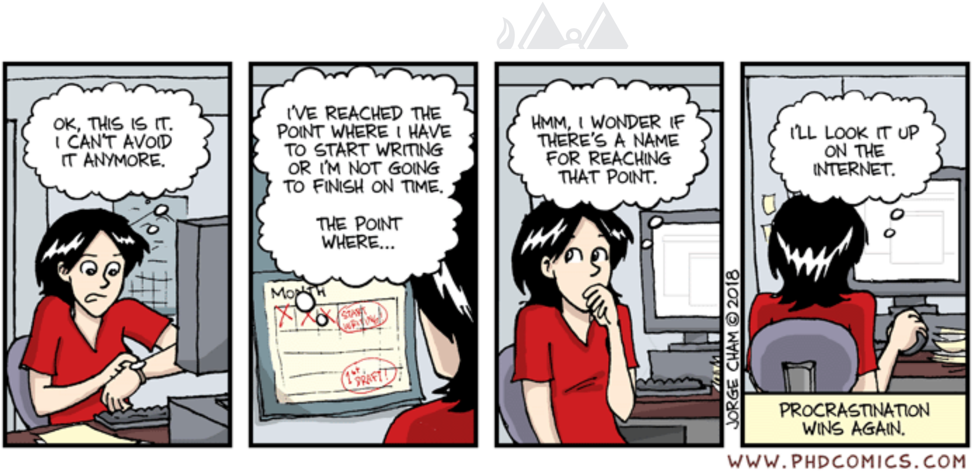
Assessment Assess results and briefly state the broadly interesting conclusion

Summary

These slides offer a few pointers towards structuring the writing of a relatively compact literature view as required for term papers

- Possible structure of the paper
- Organising the paper around research questions
- Literature sources
- Citations and referencing styles

Remember the Deadline (24 March 2023)


OK, THIS IS IT. I CAN'T AVOID IT ANYMORE.
I'VE REACHED THE POINT WHERE I HAVE TO START WRITING OR I'M NOT GOING TO FINISH ON TIME.
THE POINT WHERE...
MONTH
START WRITING
1st DRAFT!
HMM, I WONDER IF THERE'S A NAME FOR REACHING THAT POINT.
I'LL LOOK IT UP ON THE INTERNET.
PROCRASTINATION WINS AGAIN.
JORGE CHAM ©2018
WWW.PHDCOMICS.COM

Writing Term Papers

Stephen D. Wolthusen

Introduction

Referencing

Literature Sources

Plagiarism

Structure

16 Conclusions

Information Security Group