



TECHNISCHE
UNIVERSITÄT
DARMSTADT

TITLE

NAME OF THE STUDENT

Master Thesis

April 24, 1337

Secure Mobile Networking Lab
Department of Computer Science



Title

Master Thesis

SEEMOO-MSC-0000

Submitted by Name of the Student

Date of submission: April 24, 1337

Advisor: Prof. Dr.-Ing. Matthias Hollick

Supervisor: Marc Werner and Matthias Schulz

Technische Universität Darmstadt
Department of Computer Science
Secure Mobile Networking Lab

ABSTRACT

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

ZUSAMMENFASSUNG

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

CONTENTS

| | | |
|------------|-----------------------------------|-----------|
| I | INTRODUCTION | 1 |
| 1 | INTRODUCTION | 3 |
| 1.1 | First Section | 3 |
| 1.1.1 | Referencing | 3 |
| 1.1.2 | Acronyms | 3 |
| 1.1.3 | Examples on Figures | 4 |
| 1.2 | Margin Notes | 4 |
| 1.3 | Some Example Text | 4 |
| 2 | RELATED WORK | 7 |
| II | CONTRIBUTION | 9 |
| 3 | DESIGN | 11 |
| 4 | IMPLEMENTATION | 13 |
| 5 | EVALUATION | 15 |
| III | DISCUSSION AND CONCLUSIONS | 17 |
| 6 | DISCUSSION | 19 |
| 7 | CONCLUSIONS | 21 |
| IV | APPENDIX | 23 |
| A | APPENDIX | 25 |
| | BIBLIOGRAPHY | 27 |

LIST OF FIGURES

| | | |
|----------|---------------------------------------|---|
| Figure 1 | The wiretap channel | 4 |
| Figure 2 | Caption for list of figures | 5 |

LIST OF TABLES

LISTINGS

ACRONYMS

SNR signal-to-noise ratio

Part I

INTRODUCTION

The first chapter of this part gives an introduction and a motivation to this thesis, followed by a presentation of related work found in the area of physical layer security. In the third chapter, we present some definitions and background information to make it easier for the reader to quickly understand the subsequent parts of this thesis.

INTRODUCTION

Start a chapter with text and not with a section header. Open the *classicthesis-config.tex* file to insert the title of your thesis, the names of your supervisors and the hand-in date of your thesis.

1.1 FIRST SECTION

After a section there should always be text before the next section. The first paragraph is always without indentation. Starting from the second paragraph, there is an indentation.

Here is an equation without numbers for referencing:

$$\underbrace{\begin{pmatrix} \mathcal{B}_1 \\ \mathcal{B}_2 \\ \vdots \\ \mathcal{B}_R \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} H_{1,1} & H_{1,2} & \dots & H_{1,T} \\ H_{2,1} & H_{2,2} & \dots & H_{2,T} \\ \vdots & \vdots & \ddots & \vdots \\ H_{R,1} & H_{R,2} & \dots & H_{R,T} \end{pmatrix}}_{H_{\mathcal{A} \rightarrow \mathcal{B}}} \cdot \underbrace{\begin{pmatrix} \mathcal{A}_1 \\ \mathcal{A}_2 \\ \vdots \\ \mathcal{A}_T \end{pmatrix}}_{\mathcal{A}}$$

Here is an equation that you can reference:

$$\underbrace{\begin{pmatrix} \mathcal{B}_1 \\ \mathcal{B}_2 \\ \vdots \\ \mathcal{B}_R \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} H_{1,1} & H_{1,2} & \dots & H_{1,T} \\ H_{2,1} & H_{2,2} & \dots & H_{2,T} \\ \vdots & \vdots & \ddots & \vdots \\ H_{R,1} & H_{R,2} & \dots & H_{R,T} \end{pmatrix}}_{H_{\mathcal{A} \rightarrow \mathcal{B}}} \cdot \underbrace{\begin{pmatrix} \mathcal{A}_1 \\ \mathcal{A}_2 \\ \vdots \\ \mathcal{A}_T \end{pmatrix}}_{\mathcal{A}} \quad (1)$$

1.1.1 Referencing

Take a look in the following list to reference sections, figures and equations:

- Section 1.1
- Figure 1
- Equation 1

1.1.2 Acronyms

For acronyms you should use the *glossaries* package and put your acronyms in the *FrontBackmatter/acronyms.tex* file. The first acronym

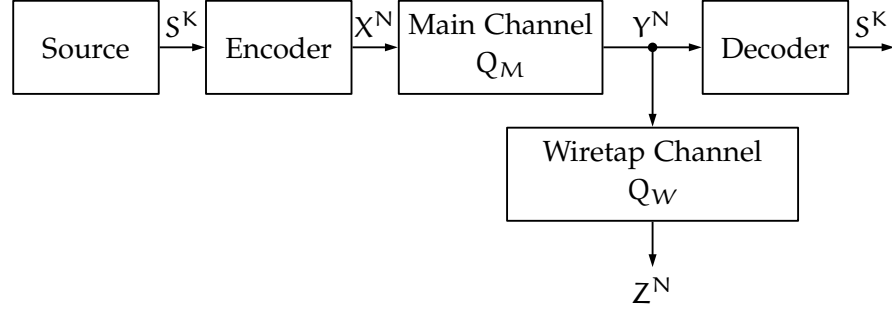


Figure 1: The wiretap channel (source: [1])

is always written in it's long form, the following occurrences are abbreviated: first occurrence signal-to-noise ratio (SNR), second occurrence SNR, plural SNRs.

1.1.3 Examples on Figures

When using figures, use vector graphics whenever possible. In Figure 1 and Figure 2 are some examples to generate vector graphics directly from \LaTeX code. The second example is based on the `matlab2tikz` script for matlab. You find an example in the `gfx/matlab/create_example_graph.m` file. TikZ is used to generate the graphics. As it takes some time and memory to recompile a graphic, pdf \LaTeX caches generated figures when the `--enable-write18` switch is set when calling pdf \LaTeX . Graphics are only recompiled when you uncomment the `\tikzset{external/remake next}` command. Figures should always appear after the first reference in the text or at the top of the same page as the reference, but never before the reference. Prefer placing figures on separate pages. Try to always have figures and text on each page. Or place enough figures to fill a page only with figures.

1.2 MARGIN NOTES

Especially in the standard SEEMOO template with wide margins, you are encouraged to insert text into the margins. If you decide to do so, plan to have at least one margin note per double page.

*Here you can add
text to the margin.
For example, to
summarize the
section next to it.*

1.3 SOME EXAMPLE TEXT

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula,

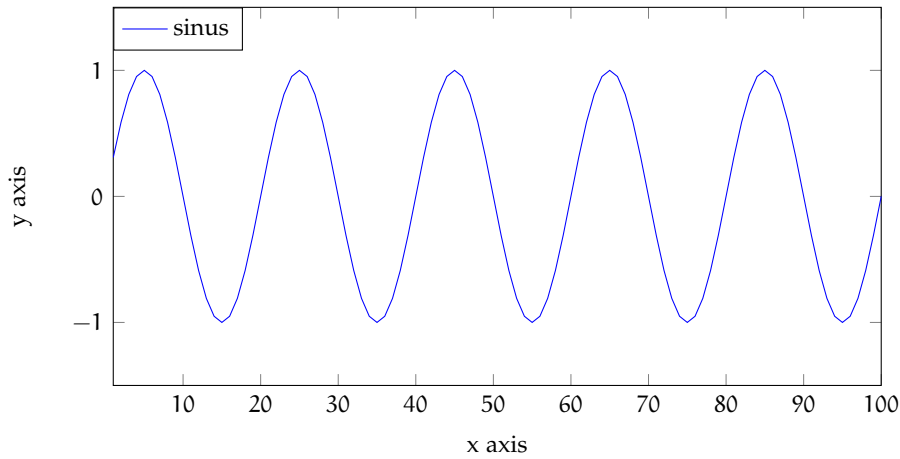


Figure 2: Caption of figure

eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetur at, consectetur sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac

habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consecratur a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consecratur. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consecratur odio sem sed wisi.

RELATED WORK

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetur adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Part II

CONTRIBUTION

The contribution starts with a design chapter, where we mathematically describe the design of the physical layer security system, as well as the adaptive filter of the attacker. After the design follows the implementation on WARP nodes. Here we give an insight into the challenges of implementing the designed MIMO communication system. The last chapter concentrates on evaluating the performance of our proposed attack in simulation and practice.

DESIGN

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetur a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consectetur. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

IMPLEMENTATION

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetur adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

EVALUATION

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetur.

Part III

DISCUSSION AND CONCLUSIONS

After the evaluation, we further discuss the results and give an outlook. In addition, we finish this work with conclusions.

DISCUSSION

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

CONCLUSIONS

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Part IV

APPENDIX

APPENDIX

Pellentesque habitant morbi tristique senectus et netus et malesuada
fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet,
egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae
justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, con-
sectetuer at, consectetur sed, eleifend ac, lectus. Nulla facilisi. Pel-
lentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse
platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet,
placemat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu,
malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis,
ultrices a, dui.

BIBLIOGRAPHY

- [1] A. D. Wyner. "The Wire-tap Channel." In: *Bell Systems Technical Journal* 54.8 (1975), pp. 1355–1387.

ERKLÄRUNG

Hiermit versichere ich gemäß der Allgemeinen Prüfungsbestimmungen der Technischen Universität Darmstadt (APB) § 23 (7), die vorliegende Masterarbeit ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus den Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, 24. April 1337

Name of the Student