基于预测的自动驾驶 GNSS 欺骗攻击检测

David Pritchard
davidpritchard.org

Gregory S. Macfarlane, Ph.D.

Chieh (Ross) Wang, Ph.D., Corresponding Author
cwang@ornl.gov

Word Count: 10 words + 1 table(s) × 250 = 260 words

Submission Date: 2022 年 3 月 14 日

ABSTRACT

全球导航卫星系统（GNSS）使用卫星与无线电通信为自动驾驶汽车（AV）提供定位、导航和定时（PNT）服务。然而，由于缺少信号加密，同时 GNSS 粗提取码（C/A）的具有公开可获得性，以及 GNSS 信号较低的信号强度，GNSS 很容易受到欺骗性攻击，从而使得 AV 的导航能力受到损害。欺骗性攻击往往很难被发现，因为欺骗者（实施欺骗性攻击的攻击者）可以模仿 GNSS 信号并向 AV 传输不准确的位置坐标。在这项研究中，我们利用长短期记忆（LSTM）模型（一种循环神经网络模型）开发了一种基于预测的欺骗攻击检测策略。LSTM 模型常被用来预测自主车辆的两个连续位置之间的距离，为了开发 LSTM 预测模型，在本项研究中，我们将使用一个名为 comma2k19 的公开真实世界驾驶数据集。该训练数据集包含不同的特征（即加速度、方向盘角度、速度和两个连续位置之间的行驶距离），这些特征是从汽车的控制区域网络（CAN）、GNSS 模块和惯性测量单元（IMU）传感器中提取的。根据对自主车辆当前位置和下一个位置之间的行驶距离进行预测，利用 GNSS 设备的定位误差和当前位置域下一个位置之间行驶距离的预测误差（即最大绝对误差），建立一个阈值。我们的分析显示，基于预测的欺骗性攻击检测策略可以成功且实时地检测到攻击。

关键词: GNSS，自动驾驶汽车，网络安全，欺骗性攻击，LSTM

INTRODUCTION

The **?** (**?**) has unique and somewhat arbitrary requirements for papers submitted for review and publication. While the initial submission is required to be in PDF format, submissions for publication in Transportation Research Record must be in Microsoft Office format. On top of this, the manuscripts must be line-numbered, captions are bolded and employ atypical punctuation, and the references must be numbered when cited and then printed in order. More details about the manuscript details can be found online at `http://onlinepubs.trb.org/onlinepubs/AM/InfoForAuthors.pdf`.

It is assumed that the readers of this document have some significant level of experience in LaTeX and `bibtex`. As use of literate programming becomes more widespread in engineering and planning, it is possible that this template may need to be made more robust.

History

David Pritchard posted the original versions of this template in 2009 and updated it in 2011, soon after TRB began allowing PDF submissions. Gregory Macfarlane made significant adaptations to it in March 2012, allowing for Sweave integration and automatic word and table counts. Ross Wang automated the total word count and made some formatting modifications in July 2015. Version 2.1.1 has been made available on GitHub in January, 2016. Version 3.1 has been made available on Github (`https://github.com/chiehrosswang/TRB_LaTeX_rnw`) in June, 2017. Versions 2.1.1 Lite and 3.1 Lite were made available on GitHub (`https://github.com/chiehrosswang/TRB_LaTeX_tex`) in June, 2017 for users who do not need R and Sweave functions provided in the original verions.

FEATURES

The template has a number of features that enable quick and painless manuscript authoring.

Title Page

The standard LaTeX `\maketitle` command is not very versatile, so we have replaced it with a `titlepage` environment. This means that the writers will be required to manually enter spacings based on the number of contributors, but the current settings (12pt between authors, 36pt before, and 60pt after them) seems to work well.

Near the bottom of the title page, TRB requires a count of the manuscript's words, figures, and tables. This template generates these counts automatically. The figure and table counts are simply pulled from the LaTeX counters using the `totcount` package. The word count feature is not as straightforward, as it utilizes a call to the system command `texcount`. Thus to compile the document writers must enable `\write18` in their `pdflatex` call.

In the newest version of this template, we added the total count automatically. The total count basically adds not only the word count, but also the equivalent count (250 words) for each table. Note that starting from 2018, Figures no longer count toward total word counts. However, each paper can have only up to 6 figures in total. The total word count is implemented using a customized command `\totalwordcount`. Please see the original code for more information.

Page Layout

The document has 1 inch margins as required, with the author's names in the left heading and the page number in the right. The authors heading will need to be edited by the writers; automating this from the title page command is not currently possible. Paragraphs leading sections and subsections are not indented, while all subsequent paragraphs in that section are. Section types are defined as outlined by the **?** (**?**).

The document is single-spaced in 12 point Times font. Times New Roman is a proprietary font and is therefore not available by installation in open-source software. While the differences between Times variants are negligible, Times New Roman itself can be used in Mac OSX by compiling under `xelatex`.

Line Numbers

Manuscript line numbering is implemented using the `lineno` package. There are options to change the font style and type, but the current settings work well. Note that the line numbers refresh each page, and that blank lines do not receive a number. Currently, line numbers and headers are not shown on the title page, but can be easily added by adding `\pagewiselinenumbers` command right before the beginning of the title page.

CAPTIONS

Figure 1 shows a Gumbel distribution as an example of captioning. As demonstrated, figure captions ought to be sentence capitalized, balded, and can be somewhat longer than in other journals.

Table captions are somewhat different, requiring initial capitals and are more of a title. An example of this is given in Table 1, showing the history of this template.

TABLE 1 A History of this Template

Version	Date	Author	Contributions
1.0	Sep 2009	Pritchard	Initial work
1.1	Mar 2011	Pritchard	Captions
2.0	Mar 2012	Macfarlane	Automation, documentation
2.1	Jul 2015	Wang	More automation and formatting
2.1.1	Jan 2016	Wang	Minor modifications and uploaded to Github
2.1.1 Lite	Jun 2017	Wang	TEX-only template
3.1	Jun 2017	Wang	Addition of `trbunofficial.cls`
3.1 Lite	Jun 2017	Wang	Addition of `trbunofficial.cls`
4.0 Lite	Jul 2019	Wang	Word count updates for Overleaf/ShareLaTeX compatibility

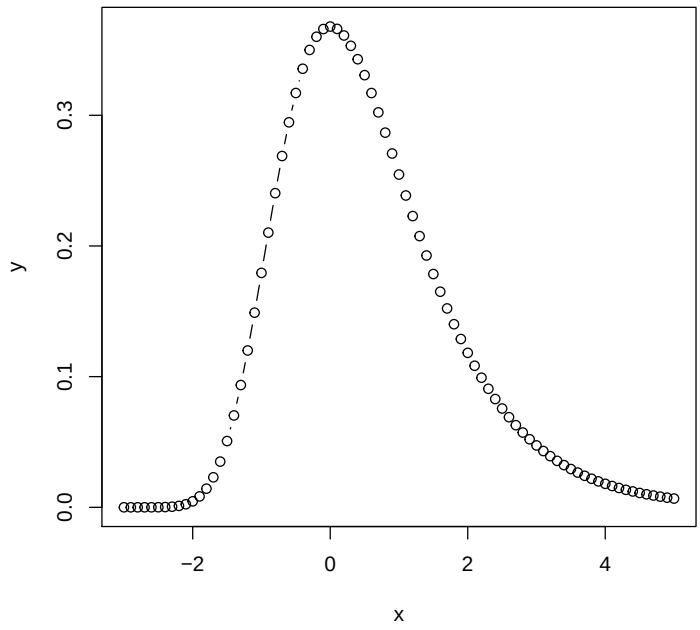

FIGURE 1 This is a random figure to test the counting functionality on the title page. It shows a Gumbel distribution with mode 0 and scale 1. The multinomial logit model assumes that the error terms are distributed identically and independently following this pattern.

Bibliography

The TRB bibliography style is defined in the `trb.bst` file which should be in your document folder. A renewed command is specified, `\citep{}` which will print the authors and the number of the reference in the order in which it is supplied. Note that `\citep{}` prints both the author names and the reference number, if you simply need the number of the reference, use command `\cite{}`. The References section will be appended to the end of the document.

It is very easy to add reference to papers programs written by **?** (**?**) and **?** (**?**) or to papers like those written by **?** (**?**) and **?** (**?**). You can even go back and refer to Biogéme by **?** (**?**) a second time. You can also cite a group of similar references without printing author names (**? ?**). This template also groups multiple reference numbers together if there are three or more consecutive numbers (**? ? ? ?**).

Equations

Intelligent driver model equations from wikipedia (`https://en.wikipedia.org/wiki/Intelligent_driver_model`) moved to the left using `amsmath` package with `fleqn` options.

$$\dot{x}_\alpha = \frac{\mathrm{d}x_\alpha}{\mathrm{d}t} = v_\alpha \tag{1}$$

$$\dot{v}_\alpha = \frac{\mathrm{d}v_\alpha}{\mathrm{d}t} = a\left(1 - \left(\frac{v_\alpha}{v_0}\right)^\delta - \left(\frac{s^*(v_\alpha, \Delta v_\alpha)}{s_\alpha}\right)^2\right) \tag{2}$$

$$s^*(v_\alpha, \Delta v_\alpha) = s_0 + v_\alpha T + \frac{v_\alpha \Delta v_\alpha}{2\sqrt{ab}} \tag{3}$$

TO DO'S

Two document types, extending from the `[numbered]` option, can be defined to differentiate the initial submission (i.e., with line numbers and in-line figures and tables) and the final manuscript (i.e., without line numbers and all figures and tables are attached to the end).

CONCLUSION

To make the document from source in a Unix-like OS, issue the following commands:

```
latexmk trb_template.tex -pdf -pvc -shell-escape
```

The `--shell-escape` option is required to access the command line for the word count. Normally this feature is disabled because it is a route of entry for malicious software. We promise that there is no such debilitating code in this document, and we encourage you to examine any scripts for suspicious code before permitting `pdflatex` from accessing your system.

Perl is necessary for "texcount" to work and needs a Perl interpreter e.g. [ActivePerl](`http://www.activestate.com/activeperl/downloads`).

ACKNOWLEDGMENTS

The authors would like to thank Aleksandar Trifunovic (`https://github.com/akstrfn`) for creating the `trbunofficial` class document, which has been a very helpful improvement.