A GNSS anti-spoofing algorithm based on attention scheme in synchronization network

Bo Lv*, Xinyu Miao and Zishan Liu
China Academy of Information and Communication Technology, Beijing, P.R. China

*Corresponding author e-mail: lvbo@caict.ac.cn

Abstract. A GNSS anti-spoofing algorithm based on attention scheme jointly with label smooth loss was proposed and verified under designed GNSS dataset to detect potential and complex spoofing threat in synchronization network. Moreover the experimental results verified that the proposed algorithm showed some better performance of machine learning metrics comparing to conventional ways.

1. Introduction
Synchronization network had been evolving for several years, of which the security of Global Navigation Satellite System (GNSS) server was not regarded as a priority because the clock source itself was not deemed a danger to the infrastructure [1]. However, as GNSS server in 5G synchronization network is becoming commonly deployed, the demand for GNSS security issue should be worthy of attention, particularly for some 5G-oriented applications, which may be likely to appear in open network environment such as indoor building, public utilities, highway station and so on. In essence, GNSS in civil field did not have the ability to authenticate and identify signals, which may easily suffer from GNSS jammer or simulators [2]. Therefore it was really a great challenge particularly under large-scaled synchronization network. In order to solve the problem, the basic idea was that if valid algorithm or scheme could be designed based on raw data collected from GNSS receiver or module to explore the inherent characteristics aiming to identify spoofing threat. It was known that in recent years great progress had been made in several areas of anomaly detection, camouflage recognition and so on adopting machine learning method, with significant advantages in multi-dimensional signal analysis and complex feature mining. Based on the above considerations, in this paper, inspired by attention scheme of transformer model [3], a GNSS anti-spoofing algorithm is proposed and discussed in synchronization network. Firstly actual GNSS data was collected via GNSS receiver while GNSS anti-spoofing dataset was further designed, secondly attention-based model as feature embedding and classifier is proposed and implemented, and finally this algorithm is verified and compared with some conventional machine learning or deep learning method such as random forest and artificial neural network (ANN).

2. GNSS dataset preparation
As is shown in Figure.1 (a), original GNSS signal was collected via GNSS receiver to generate log data, uploaded to FTP server with CGGTTS standard files [4] including some meaningful fields, e.g. running time (see STTIME in Figure.1 (b)), Transmission delay, positioning information and direction angle parameters etc., while raw data was further processed as data-frame format of which typical samples of GNSS dataset with 915944 rows and 49 columns are illustrated in Figure. 1 (b). It is noted that SAT
indicates both GNSS satellite type such as GPS/GLONASS/Beidou and channel number for specific satellite which can be used to identify individual characteristics of each satellite. Based on this actual GNSS dataset, corresponding fake data was designed as spoofing simulation results by two operations as below.

2.1. SWAP operation

Let $X_i$ represents Multidimensional feature belonging to SAT category $y_i$, a new label $z_i$ is proposed to identify if the GNSS data is tampered with spoofing device as binary value 0 or 1. \((X_i, y_i, z_i)\) is combined as a tuple while SWAP operation of data can be expressed as:

$$\begin{align*}
(X_i, y_i, z_i) &\xrightarrow{SWAP} (X_j, y_j, z_j) \\
(X_i, y_i, z_i) &\neq (X_j, y_j, z_j)
\end{align*}$$

2.2. MIXUP operation

Furthermore, in order to enhance verisimilitude of fake data, MIXUP operation is designed as:

$$\begin{align*}
(x_i, y_i, z_i) &\xrightarrow{MIXUP} (\gamma x_i + (1-\gamma)x_j, y_i, z_i) \\
(x_i, y_i, z_i) &\neq (\gamma x_i + (1-\gamma)x_j, y_i, z_i)
\end{align*}$$

Where $x_i$ refers to Continuous numeric fields picked from $X_i$, MIXUP ratio $\gamma$ is introduced to synthesis fake data.

The ultimate GNSS anti-spoofing dataset is provided with actual and spoofing GNSS dataset under above operations.

3. Framework of attention-based model for GNSS anti-spoofing

As is shown in Figure 2, an attention based model for GNSS anti-spoofing is proposed with two parts of which so-called feature embedding neural network is composed with three fully connection (FC) layers to represent feature of one GNSS data at specific STTIME, while so-called spoofing classification neural network is introduced with self-attention block and feed forward block [3] to identify inherent attribute features with residual connection [5]. It is noted that true/fake GNSS data series for $x_1^i$ to $x_N^i$ with same $y_i$ and $z_i$ sampled from continuous observation time. Accordingly two type of training loss is considered. The label smooth loss [6] is adopted to classify different category of GNSS satellite meanwhile feature similarity of true/fake data for same $y_i$ is introduced as well to avoid performing overconfidence which can be expressed as:

Figure 1. Illustration of GNSS dataset preparation.
where $K$ refers to total number of real GNSS categories in datasets and $\varepsilon$ is set as hyper parameter of label smoothing ratio to balance both true and fake data with same $y_i$ and different $z_i$. Attention operation of $f_1$ to $f_N$ is transformed from both attention block and feedback block in Figure 2 and element-wise added with skip connection block. Finally, the spoofing classification part is trained via cross entropy loss and ultimate attention model is implemented.

4. Experimental results
An experiment is designed for verification of anti-spoofing performance as binary classification based on GNSS dataset above as benchmark in this section, the result of which is implemented and computed under 2GPUs (NVIDIA P100) via Pytorch 1.1.0, compared with conventional algorithm such as Catboost, XGboost, LightBGM and ANN as well, trained and tested in Huawei NAIE platform [7] with Auto-ML scheme to obtain best performance with specific epochs. As is shown in Table 1, our algorithm is evaluated with better performance comparing to both conventional decision tree algorithm and neural network with FC blocks, for the reason that features extracted and activated in our proposed model can effectively identify significant difference adopting attention scheme jointly with label smooth trick. Furthermore it is noted that enhancing the length $N$ of detection windows is also effective to improving anti-spoofing performance with the trade-off of increasing the computational complexity and real-time detection delay, suggested to be carefully set according to actual operation requirements and hardware constraints.

Table 1. Experimental results of anti-spoofing performance under proposed algorithm and others.

| Algorithm     | Recall rate | Precision | F1 score |
|---------------|-------------|-----------|----------|
| Catboost      | 0.61        | 0.72      | 0.66     |
| XGboost       | 0.66        | 0.71      | 0.68     |
| LightBGM      | 0.74        | 0.76      | 0.75     |
| ANN(5 layers) | 0.68        | 0.77      | 0.72     |
| Ours($N=32$)  | 0.77        | 0.82      | 0.79     |
| Ours($N=64$)  | 0.81        | 0.84      | 0.82     |
5. Conclusion
In this paper a GNSS anti-spoofing algorithm based on attention model with deep learning method is put forward. This algorithm is proposed to be integrated into data processing module in GNSS receiver or monitoring system, without upgrading hardware as a software-defined and big data solution compatible with existing devices and networks. Moreover GNSS dataset provided in this paper is also recommended as GNSS anti-spoofing benchmark dataset for testing and optimizing anti-spoofing algorithm particularly in synchronization network.

Acknowledgments
This work was financially supported by National Natural Science Foundation of China (No. 62006248).

References
[1] Karen O’Donoghue, “Emerging Solutions for Time Protocol Security”, IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), (2016), pp.1-6.
[2] https://www.made-in-china.com/factory/gps-jammer.html.
[3] Ashish Vaswani, Noam Shazeer, et al., “Attention Is All You Need”, 31st Conference on Neural Information Processing Systems (NIPS 2017), (2017), pp.1-15.
[4] Wei Huang, Pascale Defraine, “BeiDou Time Transfer With the Standard CGGTTS”, IEEE Trans Ultrason Ferroelectr Freq Control, 63(2016), pp. 5-12.
[5] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun., “Deep residual learning for image recognition”, In Proceedings of the IEEE conference on computer vision and pattern recognition, (2016), pp.770-778.
[6] Rafael Müller, Simon Kornblith, Geoffrey Hinton, “when does label smoothing help?”, 33st Conference on Neural Information Processing Systems (NIPS 2019), (2019), pp.1-13.
[7] https://www.hwtelcloud.com/.