SCIENCE CHINA
Information Sciences

• LETTER •

September 2025, Vol. 68, Iss. 9, 190311:1–190311:2
https://doi.org/10.1007/s11432-024-4497-5

Special Topic: Cohesive Clustered Satellites System for 5GA and 6G Networks

Self-evolving detection of uncovered protocol attacks in 5GA and 6G NTNs

Sijia LI[1], Qian SUN[2,3*], Tianbin DANG[4], Shuzheng LIU[2], Yangliu HU[4], Lin TIAN[2,3] & Jianwei LIU[1*]

[1]*School of Cyber Science and Technology, Beihang University, Beijing 100191, China*
[2]*Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China*
[3]*Nanjing Institute of InforSuperBahn, Nanjing 211100, China*
[4]*Henan Institute of Advanced Technology, Zhengzhou University, Zhengzhou 450001, China*

Received 29 November 2024/Revised 20 March 2025/Accepted 12 June 2025/Published online 14 August 2025

Citation Li S J, Sun Q, Dang T B, et al. Self-evolving detection of uncovered protocol attacks in 5GA and 6G NTNs. Sci China Inf Sci, 2025, 68(9): 190311, https://doi.org/10.1007/s11432-024-4497-5

Nonterrestrial networks (NTNs), with the advantages of comprehensive coverage, mobility, and resilience to severe natural disasters, are being designed for fifth-generation advanced (5GA) and sixth-generation (6G) systems [1]. With the rapid advancement of ultra-dense low Earth orbit constellations and cost-effective aerospace manufacturing, the cohesive clustered satellite (CCS) system has emerged as a promising solution for 5GA and 6G NTNs. This system enables information interconnection, cooperative control, and resource sharing among base stations (BSs) and core networks (CNs) [2].

In 5GA and 6G NTNs, protocols are crucial for defining communication rules between NFs to ensure efficient and reliable data transmission. However, space NFs are especially vulnerable to malicious protocol traffic from terrestrial user equipment (UE) in unprotected coverage areas. This malicious protocol traffic can infiltrate the space CN through satellite BS clusters, paralyzing the entire space network [3].

Although anomaly detection based on deep learning (DL) effectively classifies and stops protocol traffic attacks in the CCS of 5GA and 6G NTNs, detecting and classifying uncovered protocol attacks remains challenging. Uncovered protocol attacks are novel protocol-based attacks that evade existing detection mechanisms, rule repositories, and known attack patterns. Baseline-based detection excels at identifying such uncovered attacks, whereas rule-based detection is proficient in classifying known threats. Thus, integrating these capabilities is promising for detecting and classifying uncovered attacks.

This study proposes a self-evolving detection (SED) method for uncovered protocol attacks in 5GA and 6G NTNs. SED integrates rule-based and baseline-based detection methods, ensuring tight cooperation rather than a simple concatenation. The framework detects uncovered attacks using both methods, perceives fingerprint features during baseline-based detection, and self-evolves rule-based detection to classify these attacks. A perceiving baseline detection method was designed using explainable artificial intelligence (XAI) to reveal deviation features between uncovered attacks and the normal protocol baseline, thereby extracting fingerprint features. A self-evolving rule-based detection method incorporating a self-attention mechanism can adaptively focus on protocol features to classify uncovered attacks. The proposed SED was validated with a protocol attack case and the CICIDS2017 dataset.

Threat model and case. In 5GA and 6G NTNs, the space segment is vulnerable to significant protocol threats, which often originate from malicious traffic generated by UE located in remote and distributed ground areas with inadequate protection. This malicious traffic can penetrate the CN of satellite clusters through distributed satellite BS clusters, potentially paralyzing the entire space-based network. For example, in a protocol attack targeting a space user plane function (UPF), the UPF is flooded with a massive number of requests from the attacking UE units, which are configured with high transmission rates and large payload sizes, rendering the UPF incapable of handling legitimate UE services.

SED framework. The proposed SED framework for uncovered protocol attacks in 5GA and 6G NTNs consists of a perceiving baseline detection module and a self-evolving rule detection module, as shown in Figure 1. These modules work synergistically to classify uncovered protocol attacks by perceiving and learning from their fingerprint features. During training, a wide range of fingerprint features of known attacks can be obtained from the extensive open-source datasets and used to predefine the rule detection patterns. During prediction, baseline detection perceives the fingerprint features of uncovered protocol attacks, and rule detection adjusts the feature focus and weights of predefined patterns to ensure consistency with the perceived fingerprint features of uncovered attacks. Thus, the uncovered protocol attacks are classified.

* Corresponding author (email: sunqian@ict.ac.cn, liujianwei@buaa.edu.cn)

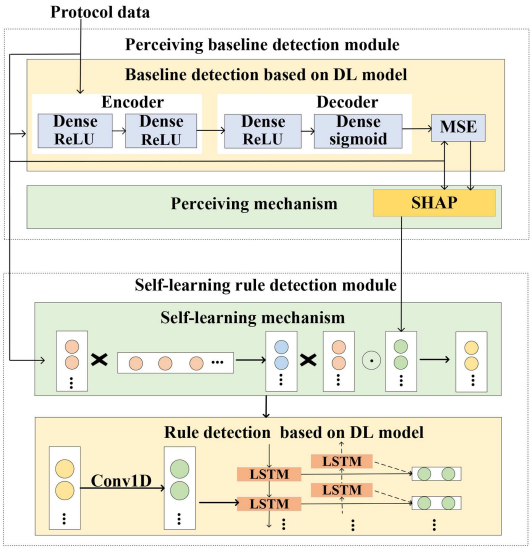

Figure 1 (Color online) Process of SED.

Perceiving baseline detection module. The perceiving baseline detection module provides a circular channel for rule detection, beginning and ending at rule detection. The input of this module comes from rule detection, which is the protocol traffic that does not match the known protocol attacks identified by the rule detection module. After detecting and perceiving the input protocol traffic, the baseline detection module outputs the perceived fingerprint features of the detected uncovered attacks to the rule detection module. Hence, the baseline detection module should be capable of detecting attacks and perceiving the fingerprint features.

To achieve this, a baseline detection model was designed based on the DL model of an autoencoder (AE) to form the baseline of normal protocol behavior. This ensured the efficient detection of attacks, including the uncovered protocol attacks. The perceiving mechanism was then designed by XAI using Shapley additive explanations to make the detection process of the baseline detection model transparent. This enables the model to determine the quantitative contributions of protocol features and then obtain the fingerprint features of the attacks, which are fed back to the rule detection module.

Self-evolving rule detection module. The SED framework begins and ends with the self-evolving rule detection module, which is designed to detect known protocol attacks and classify uncovered protocol attacks. Initially, the rule detection module filters out protocol traffic that does not match any known attack patterns. Finally, the module learns from the fingerprint features of the detected uncovered attacks, adapting the attention of the protocol features accordingly to effectively classify the uncovered protocol attacks.

For this purpose, a self-attention mechanism was placed before the rule detection model. This is the key to establishing a new classification. The rule detection model integrated a one-dimensional convolutional neural network and a bidirectional long short-term memory network (BiLSTM) to efficiently match the protocol features with the known attack patterns.

Results. The performance of the proposed SED method was evaluated with a focus on the detection and classification of uncovered attacks, the perception of baseline detection, and the self-evolution of rule detection. The data of the proposed protocol attack and the CICIDS2017 dataset were used for the evaluation.

In evaluating the detection and classification of uncovered attacks, the proposed method was compared with detection methods based on CNN-BiLSTM [4] and Hoeffding anytime tree [5]. Figure C1 shows the relationships among the detection performances of the three methods. Specifically, for uncovered attacks, Table C5 shows the detection performances. The proposed SED method outperformed the existing detection methods, detecting and classifying uncovered attacks efficiently.

Subsequently, we evaluate the perceiving capability of the baseline model and the self-evolution capability of the rule model. After the baseline model detects the uncovered protocol attacks, the perceiving mechanism attempts to capture their fingerprint features. Figures C2 and C3 show the quantitative contributions of the protocol features for the detected attacks of uncovered protocol attacks. These fingerprint features are used to adjust the focused features in rule detection. We compared the attention maps before and after self-evolution based on fingerprint characteristics, as shown in Figures C4–C6. Rule detection dynamically reassigns more attention to features with higher positive contributions and reduces attention to those with negative contributions. Thus, uncovered attacks can be detected and classified effectively.

Conclusion. An SED framework, where rule and baseline detection methods work synergistically, is proposed. The perceiving baseline detection method is designed by XAI. It reveals the deviation features between uncovered attacks and normal baselines to extract fingerprint features. The self-evolving rule detection method incorporates a self-attention mechanism to adaptively focus on the extracted fingerprint features to classify uncovered attacks. The efficiency of SED is validated with a proposed protocol attack and the CICIDS2017 dataset.

Acknowledgements This work was supported by National Key R&D Program of China (Grant No. 2021YFB2700200) and National Natural Science Foundation of China (Grant Nos. U21B2021, 61932014, 62472015).

Supporting information Appendixes A–E, Figures C1–C6, and Table C5. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Hui N, Sun Q, Zeng J, et al. Mixed numerology-based intelligent resource management in a sliced 6G space-terrestrial integrated radio access network. IEEE Trans Mobile Comput, 2025, 24: 1338–1356
2 Ma T, Qian B, Qin X, et al. Satellite-terrestrial integrated 6G: an ultra-dense LEO networking management architecture. IEEE Wireless Commun, 2024, 31: 62–69
3 Salim S, Moustafa N, Reisslein M. Cybersecurity of satellite communications systems: a comprehensive survey of the space, ground, and links segments. IEEE Commun Surv Tut, 2025, 27: 372–425
4 Nazir A, He J, Zhu N, et al. A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem. Ain Shams Eng J, 2024, 15: 102777
5 Chaitanya M, Geoffrey I W, Mahsa S. Extremely fast decision tree. In: Proceedings of ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2018. 1953–1962