LSTM-based Doppler Shift Analysis for Enhanced Security in Inter-Satellite Communications

Dogbey Ivy Selorm, Yongjae Lee, Taehoon Kim[+*], and Inkyu Bang[*]

Department of Intelligence Media Engineering, Hanbat National University

[+]Department of Computer Engineering, Hanbat National University

{isdogbey, jylee}@edu.hanbat.ac.kr, {thkim, ikbang}@hanbat.ac.kr

Abstract

This paper investigates the security challenges in a physical-layer authentication (PLA) technique that exploits Doppler shift as a unique identifier in satellite communications. Specifically, we analyze the impact of a poisoning attack on the PLA scheme for inter-satellite communications through MATLAB-based simulations.

I. Introduction

The exponential demand for mobile communication services in the limited terrestrial infrastructure and resources makes satellite communication an essential part of mobile networks. However, this unfortunately raises security threats in satellite networks.

The authors of [1] emphasized the integration of low Earth orbit (LEO) satellites within 6G networks to provide enhanced security and coverage. Further, Topal and Kurt investigated a secret key generation utilizing Doppler frequency shifts for inter-spacecraft links [2]. In satellite networks, inter-satellite links (ISL) are designed to support full networking functionality such as handover and backhaul services, but they are vulnerable to various security threats.

In this paper, we explore the performance of Doppler frequency shifts as a unique feature for inter-satellite authentication. Further, we investigate the impact of a poisoning attack on the physical-layer authentication (PLA) scheme for inter-satellite communications through MATLAB-based simulations.

II. System Model

The system model consists of a LEO constellation of N satellites per K geometric planes, as illustrated in Fig. 1. Each satellite has a link to the ground base station (GBS) and establishes ISL with any other satellites within 1 hop. The ISL is modeled as additive white Gaussian noise (AWGN), primarily affected by path loss and Doppler frequency shift [3]. Mobility information is constantly shared by connected satellites and Doppler frequency shift (DFS) is defined as follows [3]:

$$DFS = \frac{(V_t - V_r) \times (P_t - P_r)}{||P_t - P_r||},$$

where $V_t = [x_{vt}, y_{vt}, z_{vt}]$, $V_r = [x_{vr}, y_{vr}, z_{vr}]$, $P_t = [x_{pt}, y_{pt}, z_{pt}]$, $P_r = [x_{pr}, y_{pr}, z_{pr}]$ are velocity and position between transmitter and receiver at a given time, respectively.

* Corresponding Authors: Taehoon Kim and Inkyu Bang

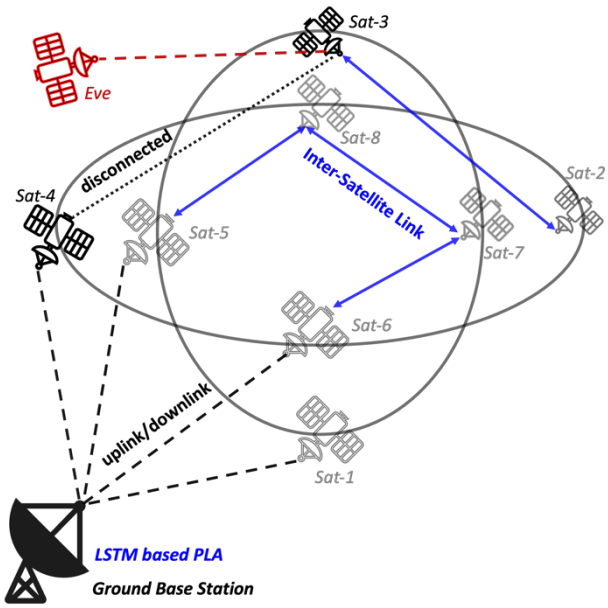

Fig. 1. System model ($N = 8, K = 2$)

Note that the ISL link is not always stable and thus an illegitimate satellite (i.e., Eve) can initiate a spoofing attack for malicious purposes when the ISL link is disconnected.

III. PLA and Poisoning Attack

For PLA, the mobility data of all satellites is collected over a duration of n days and the deep neural network is trained at the GBS. Closed Loop time series forecasting is done using long-short term memory (LSTM) layers in the model to predict velocity and position values for the next D days and the models sent to the satellites.

Using the LSTM-based PLA technique, a satellite is identified comparing predicted and actual DFS values and using the pre-determined threshold value T as follows:

$$\begin{cases} \text{legitimate one if } \mathrm{DFS}_{\mathrm{pred}} - \mathrm{DFS}_{\mathrm{act}} < T \\ \text{illegitimate one if } \mathrm{DFS}_{\mathrm{pred}} - \mathrm{DFS}_{\mathrm{act}} > T \end{cases}$$

To evaluate the performance of LSTM-based PLA techniques, we consider the following three performance metrics: root mean square error (RMSE), true positive rate (TPR), and true negative rate (TNR). Note that we consider TNR as the spoofing detection rate.

Remark: Machine learning based scheme is vulnerable to the injection of false samples during training procedures. Accordingly, we investigate the impact of the poisoning attack on the LSTM-based PLA technique by injecting noise samples into the training data.

IV. Simulation Results

In this section, we present the implementation of the system, and the detailed analysis of the numerical results.

We perform simulations with MATLAB using the 'Adam' solver, max epoch of '300', learning drop factor of 0.25, and an initial learning rate of 0.006. Employed LSTM architecture is depicted in Fig. 2.

Fig. 2. LSTM architecture

Fig. 3. Shows the RMSE for the predicted DFS values. The error increases as the days progress due to the closed loop approach used.

Fig. 4. Shows the TPR with average accuracy of 99.92% for day 1 reducing to 84.05% for day 5 due to RMSE.

Fig. 5. Shows the TPR for satellites when satellite 1 has been affected by poisoning attack of 10% of satellite 1's training samples. The attacker's velocity is chosen to be a random value between the minimum and maximum velocity of satellite 1, and its position is also random within a 10km to 100km vicinity of the receiver. The attack degrades the average accuracy of satellite 1 from 98.32% to 52.41%.

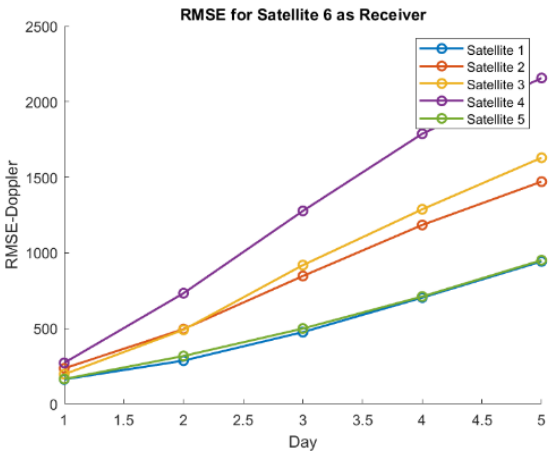

Fig. 3. RMSE of Doppler frequency shift

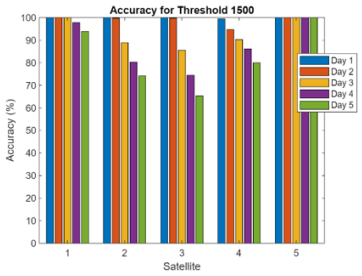

Fig. 4. Authentication accuracy testing ($T = 1500\ Hz$)

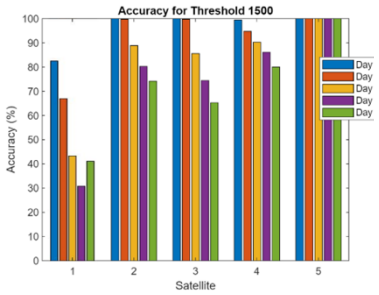

Fig. 5. Degradation of authentication accuracy under poison attack ($T = 1500\ Hz$)

V. Conclusion

Our work analyzed the application of Doppler frequency shift as a feature for authentication in inter-satellite links. The approach is vulnerable to a poisoning attack, which can be mitigated by training the model with previous Doppler frequency shift values rather. This remains for future work.

ACKNOWLEDGEMENT

This research was supported by the MSIT(Ministry of Science, ICT), Korea, under the National Program for Excellence in SW), supervised by the IITP(Institute of Information & communications Technology Planing & Evaluation) in 2024 (2022-0-01068) and also partially supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1F1A1076126).

REFERENCES

[1] Z. Xiao, et al., "LEO Satellite Access Network (LEO-SAN) Toward 6G: Challenges and Approaches," in *IEEE Wireless Communications*, vol. 31, no. 2, pp. 89-96, 2024.

[2] O. A. Topal and G. K. Kurt, "Securing the Inter-Spacecraft Links: Physical Layer Key Generation from Doppler Frequency Shift," in IEEE Journal of Radio Frequency Identification, vol. 5, pp. 232-243, 2021.

[3] O. A. Topal and G. K. Kurt, "Physical Layer Authentication for LEO Satellite Constellations," in 2022 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1952-1957, 2022.