Sensor-based Threats to AI enabled Next Generation Aircraft Maintenance

Gautam Raj Mode and Khaza Anuarul Hoque

Dependable Cyber-Physcial Systems (DCPS) Laboratory
Department of Electrical Engineering & Computer Science, University of Missouri-Columbia, USA

Motivation

- Aircraft engine manufacturers, such as Rolls Royce is developing **AI** enabled next generation aircraft engines, which uses **Engine health monitoring (EHM)** to monitor the health of the engine based on the concept of **predictive maintenance (PdM)** [4].
- An EHM system employs several **IoT** sensors to collect different parameters of the engine and **Machine learning (ML)** algorithms to monitor the health.
- However, ML algorithms are prone to threats, knows as **adversarial machine learning** [1, 5] which is a technique to fool ML models through malicious input. In addition, IoT sensors in EHM systems, inherit a wide variety of cyber-attacks [3], which possess a vital threat for an aircraft's PdM.
- It constitutes a novel **Adversarial PdM** problem. This research **explores** and **evaluates** the effect of DoS, Replay and FDIA attack on a **deep learning** based EHM system using NASA's Turbofan Engine Degradation Data Set [2].

Predictive maintenance for EHM

- **Remaining useful life (RUL)** is the length of time a machine is likely to operate before it requires repair or replacement.

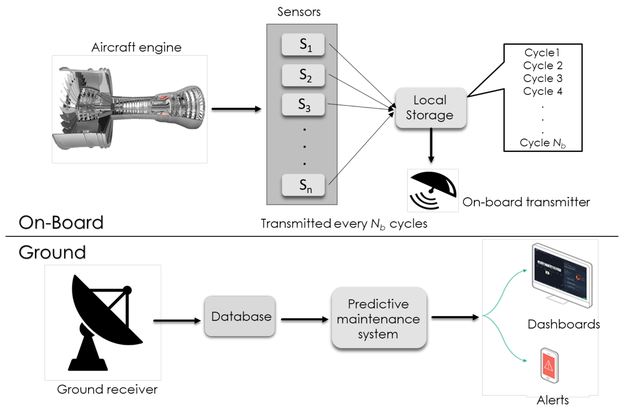

Fig. 1: Engine health monitoring (EHM) system architecture

Deep learning (LSTM) network

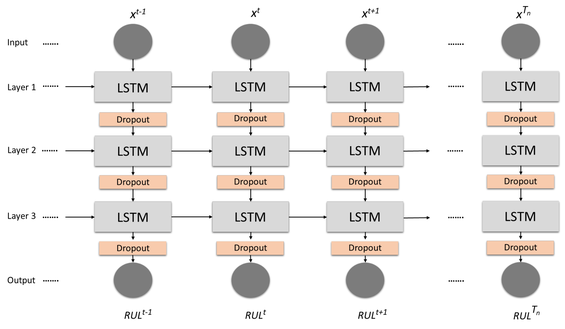

Fig. 2: Deep LSTM architecture

Cyber-attacks on a PdM system

- **False data injection attack (FDIA):** In this attack a vicious vector is added to the original vector, which modifies the sensor output by a very small margin (0.2% to 0.3%).
- **Replay attack**: The delay or repeat of the data transmission is carried out by the attacker, who intercepts the data and re-transmits it.
- **Denial of service attack (DoS)**: It can partially or entirely disrupt the data exchange between sensors and central engine control.

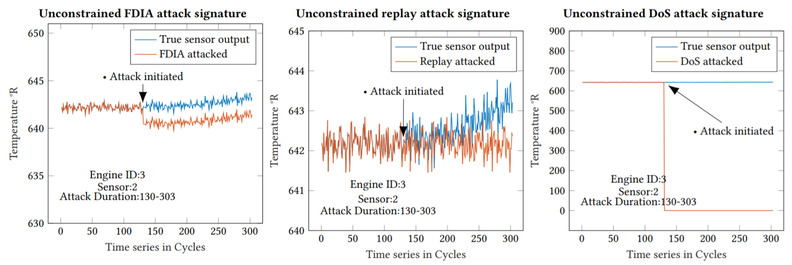

Fig. 3: Attack signatures

Impact of cyber-attacks on aircraft PdM

- **Attack scenario 1**: The attacker plants malicious sensors on board the engine during maintenance. The attacks are performed after average degradation point.
- **Attack scenario 2**: The attacker plants malicious sensors on board the engine during maintenance. The attacks from initial time cycles.
- **Attack scenario 3**: The attacker is on board the airplane. The attacks are performed for the flight duration.

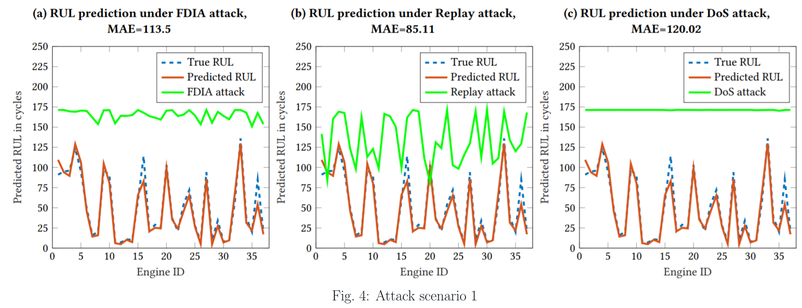

Fig. 4: Attack scenario 1

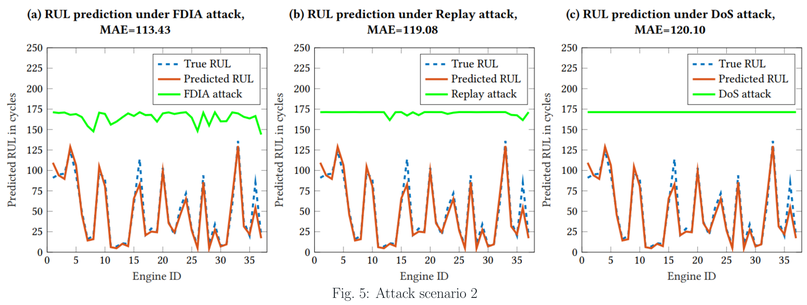

Fig. 5: Attack scenario 2

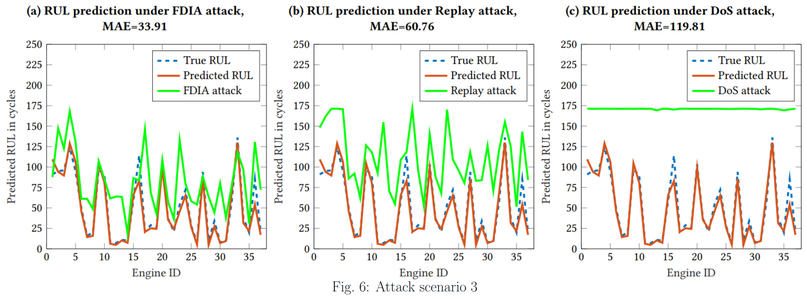

Fig. 6: Attack scenario 3

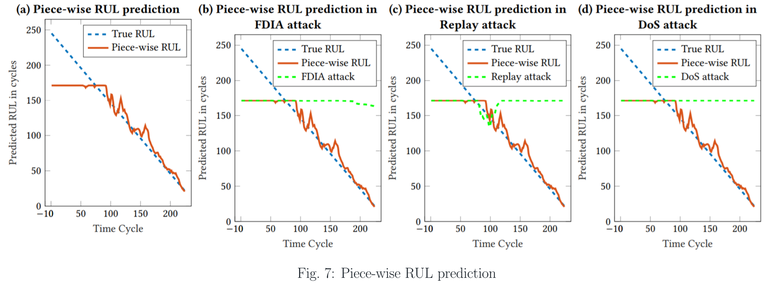

Fig. 7: Piece-wise RUL prediction

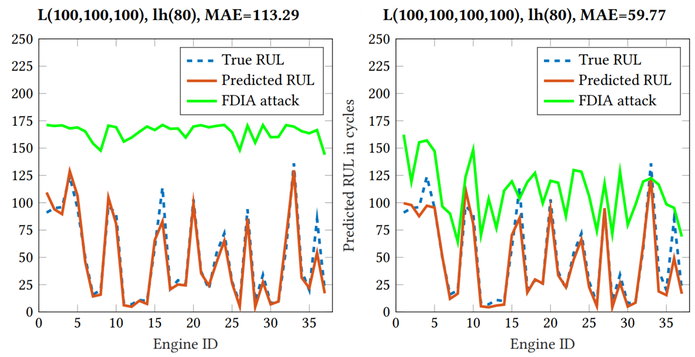

Fig. 8: Comparison of multi-layer LSTM networks under FDIA attack of scenario 2

Scenario	MAE			
	True	FDIA	Replay	DoS
1	7.26	113.5	85.11	120.2
2		113.43	119.08	120.10
3		33.91	60.76	119.81

Fig. 9: MAE comparison for attacks scenarios

Discussion

- We observe that all unconstrained attacks (complete control of the attack) have **more impact on the PdM system** in comparison to the constrained attacks (limited control of the attack).
- Both the constrained and unconstrained **DoS attacks** have a **lethal** and similar influence on the PdM system.
- From Figure 9, it can be observed that as the number of **LSTM layers increases** the network becomes more **resilient to the FDIA attack**.

Conclusions

- In this work, we first evaluate the deep learning approach in predicting aircraft engine RUL, and obtained results show a great prospect for **deep learning in PdM**. However, aircraft PdM is highly susceptible to several cyber-attacks.
- We model three different attacks (DoS, FDIA, and replay attack) on the IoT sensors that provide data to PdM system and evaluate their impacts on RUL prediction. The obtained results show that the **DoS attack** is the most lethal attack for the aircraft PdM system.
- We also show that the **number of layers** in LSTM has a direct relationship with the **FDIA attack**, e.g., increasing the number of layers in LSTM also enhances the resiliency against the FDIA attack.
- In the future, we plan to develop an end-to-end methodology for detecting and mitigating cyber-attacks in a PdM system.

References

[1] Alexey Kurakin, Ian Goodfellow, and Samy Bengio. "Adversarial machine learning at scale". In: *arXiv preprint arXiv:1611.01236* (2016).

[2] Abhinav Saxena and Kai Goebel. "C-MAPSS data set". In: *NASA Ames Prognostics Data Repository* (2008).

[3] Amit Kumar Sikder et al. "A survey on sensor-based threats to internet-of-things (iot) devices and applications". In: *arXiv preprint arXiv:1802.02041* (2018).

[4] Gian Antonio Susto et al. "Machine learning for predictive maintenance: A multiple classifier approach". In: *IEEE Transactions on Industrial Informatics* 11.3 (2015), pp. 812–820.

[5] Yevgeniy Vorobeychik and Murat Kantarcioglu. "Adversarial machine learning". In: *Synthesis Lectures on Artificial Intelligence and Machine Learning* 12.3 (2018), pp. 1–169.