Impact of False Data Injection Attacks on Deep Learning enabled Predictive Analytics

Gautam Raj Mode, Prasad Calyam, Khaza Anuarul Hoque
Department of Electrical Engineering & Computer Science
University of Missouri, Columbia, MO, USA
gmwyc@mail.missouri.edu, calyamp@missouri.edu, hoquek@missouri.edu

Abstract*—Industry 4.0 is the latest industrial revolution primarily merging automation with advanced manufacturing to reduce direct human effort and resources. Predictive maintenance (PdM) is an industry 4.0 solution, which facilitates predicting faults in a component or a system powered by state-of-the-art machine learning (ML) algorithms (especially deep learning algorithms) and the Internet-of-Things (IoT) sensors. However, IoT sensors and deep learning (DL) algorithms, both are known for their vulnerabilities to cyber-attacks. In the context of PdM systems, such attacks can have catastrophic consequences as they are hard to detect due to the nature of the attack. To date, the majority of the published literature focuses on the accuracy of DL enabled PdM systems and often ignores the effect of such attacks. In this paper, we demonstrate the effect of IoT sensor attacks (in the form of false data injection attack) on a PdM system. At first, we use three state-of-the-art DL algorithms, specifically, Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Convolutional Neural Network (CNN) for predicting the Remaining Useful Life (RUL) of a turbofan engine using NASA's C-MAPSS dataset. The obtained results show that the GRU-based PdM model outperforms some of the recent literature on RUL prediction using the C-MAPSS dataset. Afterward, we model and apply two different types of false data injection attacks (FDIA), specifically, continuous and interim FDIAs on turbofan engine sensor data and evaluate their impact on CNN, LSTM, and GRU-based PdM systems. The obtained results demonstrate that FDI attacks on even a few IoT sensors can strongly defect the RUL prediction in all cases. However, the GRU-based PdM model performs better in terms of accuracy and resiliency to FDIA. Lastly, we perform a study on the GRU-based PdM model using four different GRU networks with different sequence lengths. Our experiments reveal an interesting relationship between the accuracy, resiliency and sequence length for the GRU-based PdM models.

***Index Terms*—deep learning, false data injection attack, LSTM, GRU, CNN, industry 4.0, Internet of things, machine learning**

I. INTRODUCTION

Current advances in machine learning (ML) techniques and Internet-of-Things (IoT) sensors has enabled the emergence of predictive maintenance (PdM), which is a method of preventing asset failure by analyzing production data and identifying patterns to predict issues before they happen. State-of-the-art PdM techniques outperform the classical PdM methods [1], and can help reduce downtime by 35%-45%, maintenance cost by 20%-25%, and can increase production by 20%-25% [2]. Due to these benefits, IoT and ML-enabled PdM solutions are reshaping automotive, aerospace, oil and gas, transportation, manufacturing industries and also reshaping the national defense. Specifically, deep learning (DL) algorithms have recently shown tremendous success in such PdM applications [3]. Unfortunately, IoT sensors and DL algorithms are both susceptible to attacks [4], which poses a significant threat to the overall PdM system. According to a recent report from the *Malwarebytes*, cyber-threats against businesses/factories have increased by more than 200% over the past year [5].

Specifically, it is very hard to detect stealthy attacks, such as False Data Injection Attack (FDIA) [6] on the PdM system due to the nature of the attack. In an FDI attack [6], an attacker stealthily compromises measurements from IoT sensors (by a very small margin), such that the manipulated sensor measurements bypass the sensor's basic 'faulty data' detection mechanism and propagates to the sensor output undetected. Such attacks on a PdM system may not even show their impact immediately. Instead, the attack propagates from the sensor to the ML part of the PdM system and fools the system by predicting a delayed asset failure or maintenance interval. This might incur a significant cost by inducing an unplanned failure or loss of human lives in safety-critical applications [7]–[9].

Extensive research has been performed on the detection and mitigation of FDI attacks in cyber-physical systems (CPS) domain [10]–[12]. Unfortunately, the effect of FDIA on a PdM system is yet not explored which motivates our research. In the case of aircraft engine PdM systems, FDIAs may result in the delay of timely maintenance and lead to mid-air engine failures which are catastrophic. Current users of PdM systems for aircraft engine maintenance include Pratt and Whitney, Rolls-Royce, Honeywell, General electronics and the US Air force [7], [13]–[15]. For example, Bombardiers new jetliner uses a Pratt and Whitney turbofan engine that boasted more than 5,000 sensors [16], [17]. Powered with the modern DL algorithms, this engine can predict the future demands of the engine, perform adjustments, and thus save 15% of fuel usage. However, the vulnerability of sensor-attacks against such IoT and ML-based engines is considered a challenge [16], [18], [19]. The existing sensor attack detection solutions in the IoT and cyber-physical system domain is not sufficient to address this problem due to the fact that, when deployed individually to the thousands of sensors, most of the existing techniques suffer from scalability problems and resource overheads as many IoT sensors are power and resource-constrained.

Contribution of this paper: In this paper, we model continuous and interim FDIAs on IoT sensors and show their impact on a PdM model by performing a case study on the aircraft Predictive Maintenance (PdM) system. We use the C-MAPSS [20] (Commercial Modular Aero-Propulsion System Simulation) dataset. At first, to build an accurate predictive model, we train the Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Convolutional Neural Network (CNN) algorithms using the C-MAPSS dataset. We evaluate these three predictive models, and the obtained results show that the GRU-based model predicts the Remaining Useful Life (RUL) most accurately. The obtained results from the GRU-based model outperforms the recent works that use DL for RUL prediction using the C-MAPSS dataset in [21]–[23] (by predicting RUL 1.3-1.9 times more accurately).

Afterward, we model two types of FDI attacks on the C-MAPSS dataset and evaluate their impact on CNN, LSTM, and GRU-based PdM models. To be more realistic, we model attack only on 3 sensors (attacks that modify their readings by a very small margin) among the 21 sensors in the dataset. The obtained results show that all the PdM models are greatly defected by the FDIA even if only 3 out of the 21 sensors are attacked. However, the GRU-based PdM model is comparatively more accurate and resilient to FDIA when compared to the other evaluated PdM models. In terms of sensitivity, we also explore that CNN is way more sensitive to FDIAs when compared to the LSTM and GRU. Afterward, we analyze the GRU-based PdM model using four different sequence lengths. The obtained results show an interesting relationship between the accuracy, the resiliency and the sequence length of the models. To the best of our knowledge, this is the *first work* that demonstrates the effects of IoT sensor attacks on a deep learning-enabled PdM system.

Paper organization: The rest of the paper is organized as follows. Section II describes the modeling of FDIA in detail. Section III compares the performance of CNN, LSTM, and GRU in predicting RUL and analyses the impact on RUL prediction using CNN, LSTM, and GRU after both continuous and interim FDIA. Section IV presents the observations from those obtained results, and Section V concludes the paper.

II. Modeling of FDIA

In this section, we describe the modeling of FDIAs, attacker's objective, attack surface, and the attack scenarios in detail.

False data injection attack (FDIA): An FDI attack [6] can be injected into the system by compromising physical sensors, sensor data communication links, and data processing programs. Compromising physical sensors requires physical access to the sensors and hence is a tedious task. In contrast, hacking the sensor data communication links and data processing programs is an easier option for an attacker (explained in detail in the *attack surface* of this section). For example, X_i represents the information transmitted by the i^{th} sensor. In an FDIA, the adversary contaminates the original vector with a vicious vector. Let $X_i = [x_1, x_2, ..., x_k]$ be the original vector data containing k sensor reading for the i^{th} sensor. The original vector could be contaminated by adding an FDIA vector with the same dimension as the original vector. Let the contaminated vector for the i^{th} sensor be $F_i = [\lambda_1, \lambda_2, ..., \lambda_k]$, then the compromised vector is given by Eq. 1.

$$Z_i = X_i + F_i \tag{1}$$

In this work, we consider the constrained attack (attacker has access to a limited number of sensors) since it is more practical that an attacker has access to only a limited number of sensors. We model two variations of FDIAs to explore and compare their impact, specifically, *continuous FDIA* and *interim FDIA*. In the case of continuous FDIA, the attack is continuous, which means, once the attack starts, from that point on-wards all the sensor reading are compromised. For instance, if the attack starts at the time instant $atck\_start = 3$ and ends at $atck\_end$ then F_i can be expressed as $F_i = [\lambda_1, \lambda_2, \lambda_{atck\_start}, ..., \lambda_{atck\_end}]$, where $atck\_start \geq 1$ and $atck\_end = k$. In the case of interim FDIA, the duration of attack is a short time interval, where $atck\_start > 1$ and $atck\_end < k$.

Attacker's stealthiness: An FDIA can be stealthy if it is not detected by the defense mechanism. In order to achieve that objective, the attack vector should remain in the boundary conditions of the sensor measurements. There exist constant vectors Z_{min} and Z_{max}, such that for any FDIA vector Z_i, the compromised vector passes undetected through the defense if

$$Z_i = X_i + F_i \; and \; Z_{min} \leq Z_i \leq Z_{max} \tag{2}$$

We assume the attacker knows Z_{min} and Z_{max} to construct attack vectors satisfying Eq.2. Such information is easily available from the sensor data sheets provided by the vendor.

Attacker's objective: The attacker's objective is to cause a delay in aircraft engine maintenance. This objective can be achieved by altering the IoT sensors readings that are fed to the PdM systems. Injecting false data to the sensor readings results in incorrect predictions from PdM systems which in turn results in a delay of timely maintenance. One can argue that the attacker having access to the physical sensors or the communication network of the sensors would directly attack the main systems (flight navigation and instrument landing systems) rather than just altering the sensor values for the PdM. However, there is a higher chance that a direct attack on the main system will easily get detected by the defense mechanisms. In contrast, introducing FDIA to sensors is a safer option for an attacker since such attacks are more stealthy, hard to detect as they are in the sensor's acceptable range. Thus, such attacks will cause an erroneous calculation of the RUL and might delay the maintenance cycle leading to a catastrophic incident.

Attack surface: One of the recent articles [24] considers cyber-attacks as one of the reasons behind the two recent Boeing 737 Max 8 crashes. According to that article, a passenger, vehicle or drone carrying a sonic device capable of impacting the MCAS sensor controlling the plane could have been responsible for such an attack. Recently, ICS-CERT published an alert on certain controlled area network (CAN) bus systems aboard aircraft that might be vulnerable to hacking. It cited a report that an attacker with access to the aircraft could attach a device to avionics CAN bus to inject false data, resulting in incorrect readings in an avionic equipment [25]. Using such a device attached to the bus could lead to incorrect engine telemetry readings, incorrect compass, altitude data, airspeed, and Angle of Attack (AoA) data. Pilots might not be able to distinguish between false and legitimate readings. This alert explores the possibility of injecting false data into IoT sensor readings of aircraft engine which are transmitted on a CAN. In this work we consider FDIA using a malicious device attached to an avionics CAN. Other attack surfaces are discussed in our extended paper [26].

Attack scenario: As shown in Fig.1 in [26] of the Engine health monitoring (EHM) architecture, the aircraft sends N_b cycles of data at a time to the ground station/engine manufacturer. At the ground station, the PdM system performs data analytics on the received data and sends out alerts if the RUL is close to the threshold N_{th}. The value of N_{th} can vary from engine to engine, and it is manufacturer-dependant. An adversary having this knowledge can perform the attacks more effectively. Assuming in an engine, the linear degradation initially starts at N^d cycle. The value of N^d is different for different engines, as the wear of the engines may be different. If the average of N^d for all the engines in the dataset is taken, it is found to be N^d_{avg}. An adversary knowing N^d_{avg} can perform the attacks after the degradation initiates, making the attack more destructive.

To study the impact of FDIA on PdM systems, we consider an attack scenario where the attacker has access to the aircraft and could attach a device to avionics CAN bus [25] as mentioned previously in section II (attack surface). The device attached to CAN bus can inject false data into engine sensor readings, resulting in incorrect predictions of RUL of the aircraft engine. In this work, we consider two variations of FDIA which are continuous and interim FDIA. In continuous FDIA, the attack is initiated after N^d and continues to the end-of-life of the engine. In Interim FDIA, the attack is initiated after N^d and continues to the next 20 time cycles. In both the variations of FDIA, random and biased FDIAs are used to evaluate the PdM model's performance. Here, random FDIA means the noise added to the sensor output has a range (0.01% to 0.05%). Whereas, biased FDIA has a constant amount of noise added to the sensor output.

III. EXPERIMENTAL RESULTS

In this section, we first compare three different DL algorithms for RUL prediction. Next, we present both continuous and interim FDIA signatures, and the impact of FDIAs on the RUL prediction. Lastly, we present piece-wise RUL prediction and detail the impact of sequence length on resiliency.

A. Comparison of deep learning algorithms

In order to select the best machine learning algorithm for the PdM, we compare the performance of LSTM, GRU, and CNN algorithms for the C-MAPSS dataset. To evaluate the performance of these DL models, we utilize the root mean square error (RMSE) metric which is widely used as an evaluation metric in model evaluation studies. Table I represents the comparison of these DL algorithms with architectures LSTM(100,100,100,100) lh(80), GRU(100,100,100) lh(80), and CNN(64,64,64,64) lh(100). The notation GRU(100,100,100) lh(80) refers to a network that has 100 nodes in the hidden layers of the first GRU layer, 100 nodes in the hidden layers of the second GRU layer, 100 nodes in the hidden layers of the third GRU layer, and a sequence length of 80. In the end, there is a 1-dimensional output layer. The details about the developed LSTM, GRU and CNN models (including the hyperparameters), and the C-MAPSS dataset can be found in the extended version of this paper [26]. For the sake of reproducibility and to allow the research community to build on our findings, the artifacts (source code, datasets, etc.) of the following experiments are publicly available on our GitHub repository[1].

TABLE I: RMSE comparison for different DL algorithms

Predictor architecture	**RMSE**
	Test
CNN(64,64,64.64) lh(100)	9.94
LSTM(100,100,100,100) lh(80)	8.76
GRU(100,100,100) lh(80)	7.26

From Table I it is evident that the DL algorithm GRU(100, 100, 100) with a sequence length 80 has the least RMSE of 7.26. It means that GRU is very accurate in predicting accurate RUL for this dataset. Note, the obtained results in Table I show that our GRU-based predictive model performs 1.9, 1.7 and 1.3 times better (in terms of accuracy) when compared to the recent works in [21], [23], [27], respectively, on RUL estimation using DL algorithms and the C-MAPSS dataset.

B. Impact of attacks on a PdM system

The average degradation point of the engine N^d_{avg} is considered as 130 for the FD001 dataset [28] [29] [30], and we assume that the EHM system of the aircraft sends 20-time cycles (N_b) of data to the ground at a time. The details of EHM, the parameter N_b and how the data is sent to the ground are discussed in [26]. The FDIA can be performed on 21 sensors, but to make the attack more realistic, we perform FDIA on only 3 sensors (specifically, T24, T50, and P30). More information about these sensors can be found in [31]. In FDIA continuous scenario, the attacker has initiated the attacks after N^d_{avg}, which is 130-time cycles (a one-time cycle

[1]https://github.com/dependable-cps/FDIA-PdM

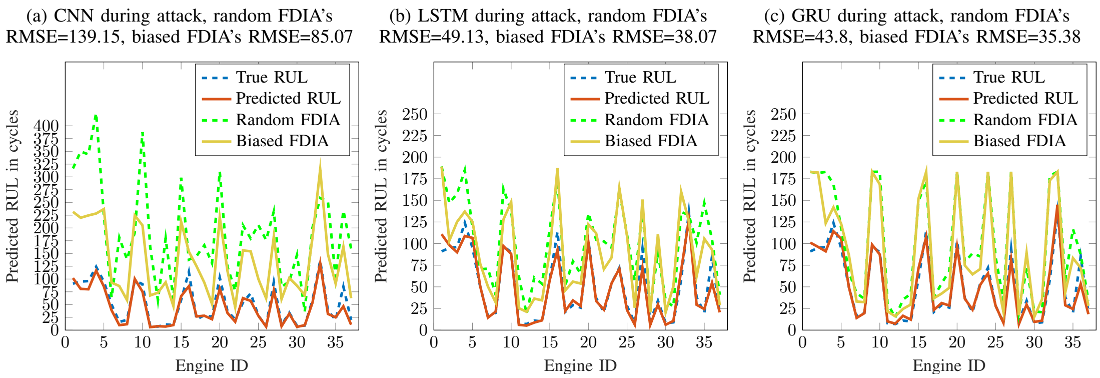

Fig. 1: FDI attack scenario for continuous period

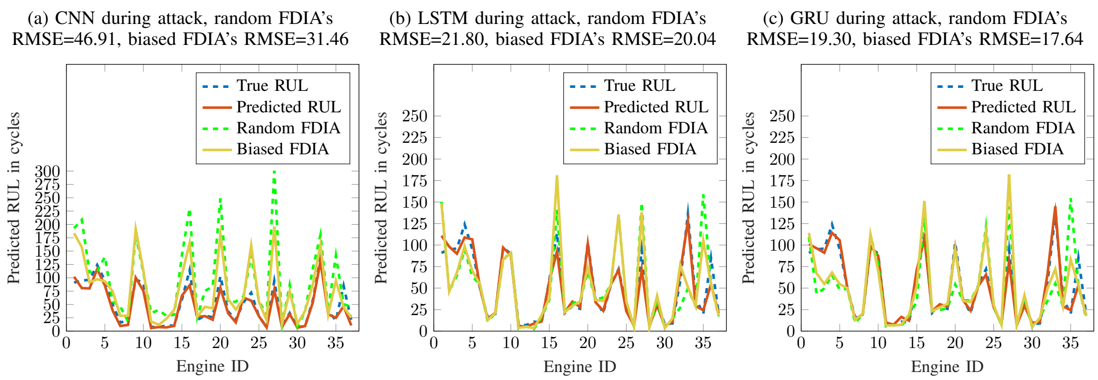

Fig. 2: FDI attack scenario for interim period

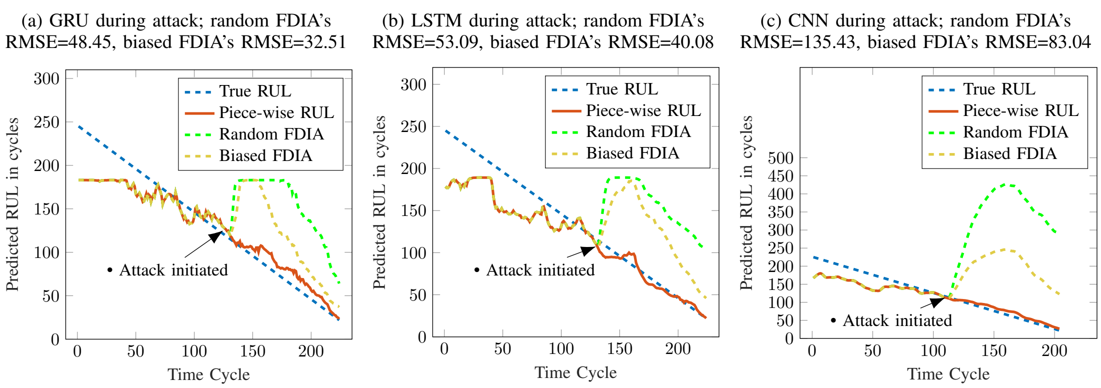

Fig. 3: Piece-wise RUL prediction for continuous FDIA

is equivalent of one flight hour), and the attack duration is until end of life of the engine. In FDIA interim scenario, the attacker has initiated the attacks after N^d_{avg}, which is 130-time cycles, and the attack duration is 20 hours (20-time cycles). Since the attack is initiated after 130-time cycles, we only consider the engines which have data for more than 130 cycles which gives us 37 engines in the FD001 dataset. The resultant dataset is re-evaluated using the LSTM, CNN and GRU-based PdM models and the obtained RMSEs are 6.09, 7.50, and 5.36, respectively.

FDIA signature: To model the FDIA on sensors, we add a vicious vector to the original vector, which modifies the sensor output by a very small margin (0.01% to 0.05%) for random FDIA and 0.02% for biased FDIA. Here, random FDIA means the noise added to the sensor output has a range (0.01% to 0.05%). Whereas, biased FDIA has a constant amount of noise added to the sensor output. The attack signatures can be found in our extended paper [26].

Impact of FDIA on CNN, LSTM and GRU: To show the impact of an FDIA on the aircraft PdM system, we implement an attack for the scenario mentioned previously in Section II (attack scenario). The FDIA is performed on three sensors (T24, T50, and P30) instead of attacking all the 21 sensors in the dataset. In FDIA continuous scenario, the adversary performs attacks from 130-time cycles to end of life of the engine. It is evident from Fig. 1 that LSTM, GRU, and CNN are greatly affected by the continuous FDI attack. In the case of random and biased FDIA, random FDIA showed a considerable impact on all PdM models. The CNN based PdM

(a) GRU during attack; random FDIA's RMSE=25.69, biased FDIA's RMSE=22.92 (b) LSTM during attack; random FDIA's RMSE=27.25, biased FDIA's RMSE=25.07 (c) CNN during attack; random FDIA's RMSE=57.42, biased FDIA's RMSE=33.99

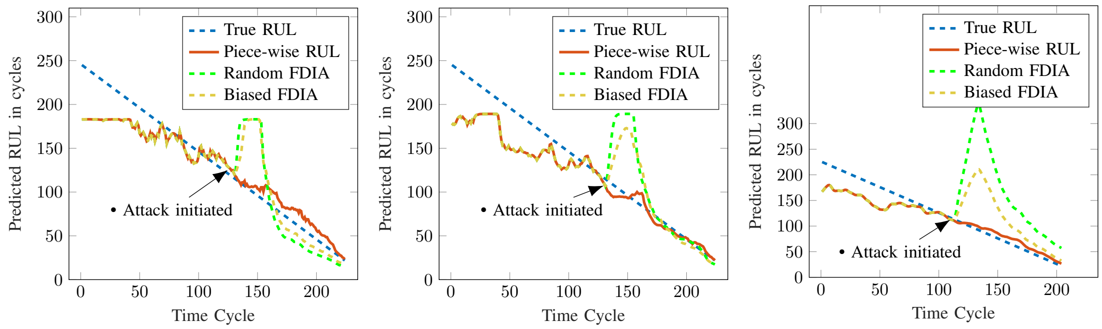

Fig. 4: Piece-wise RUL prediction for Interim FDIA

model is the most affected by the continuous FDIA as random FDIA's RMSE is 139.15 and biased FDIA's RMSE is 85.07 (true RMSE is 7.50) which is almost 18 times and 11 times higher when compared to the true RMSE, respectively. In contrast, the GRU based PdM model is the least affected by the continuous FDIA as random FDIA's RMSE is 43.8 and biased FDIA's RMSE is 35.38 (true RMSE is 5.36). Even though the GRU is least affected by both random and biased FDIA, their RMSE is 8 and 6 times higher than the true RMSE, respectively, making it also deadly for a PdM system.

In the FDIA interim scenario, the adversary performs attacks between 130 and 150-time cycles (20-time cycles). It is evident from Fig. 2 that LSTM, GRU, and CNN are greatly affected by the interim FDI attack. Once again, the CNN based PdM model is greatly affected by the continuous FDIA as random FDIA's RMSE is 46.91 and biased FDIA's RMSE is 31.46 (true RMSE is 7.50) which is almost 6 times and 4 times higher than the true RMSE, respectively. In contrast, the GRU based PdM model is the least affected by the interim FDIA as random FDIA's RMSE is 19.30 and biased FDIA's RMSE is 17.64 (true RMSE is 5.36). This indicates that GRU-based PdM models are comparatively resilient to both continuous and interim FDIA. Even though the GRU is least affected by both random and biased FDIA, their RMSE is still 4 times and 3 times higher than the true RMSE, respectively, making it deadly for a PdM system. When comparing both continuous and interim FDIA, it observed that continuous FDIA's RMSE is almost twice the interim FDIA's RMSE. Hence, continuous FDIAs are more potent than interim FDIA.

C. *Piece-wise RUL prediction*

In order to show the impact of FDIA attacks on a specific engine data, we apply the piece-wise RUL prediction. The piece-wise RUL prediction gives a better visual representation of degradation in an aircraft engine. Fig. 3(a) shows an example of an engine data from the dataset of 100 engines, and depicts the predicted RUL using GRU at each time step of that engine data. For example, if X is the time series data of a particular engine, then $X_i = [x_1, x_2, x_3 ... x_{t-k}]$ represents time series data until time $t-k$. RUL^p is predicted RUL at each time step in X, which is can be defined as $RUL_i^p = [RUL_1^p, RUL_2^p, RUL_3^p ... RUL_{t-k}^p]$. From Fig. 3(a), it is evident that as the time series approaches the end of life, the predicted RUL (red line) is close to the true RUL (blue dashes), because the DL model has more time series data to accurately predict the RUL.

In the case of piece-wise RUL prediction during continuous FDIA, it is observed from Fig. 3 that both random and biased FDIAs are initiated from 130-time cycles to 242-time cycles for engine ID 17. Here, the green and yellow dashes in the figures are predicted RUL after random and biased FDIA, respectively. In the GRU, LSTM, and CNN based piece-wise RUL prediction (for both random and biased FDIA), the attacker initiates the FDIA after 130-time cycles. The impact of the attack is quite interesting as the RUL jumps upwards (around 200 for GRU and LSTM) with a possible indication to the engine maintenance operator that the engine is quite healthy. This may influence a 'no maintenance required' decision from the maintenance engineers' point of view, however, in reality, the RUL is decreasing continuously and going below the 100-time cycles which might require to schedule urgent maintenance leading to a catastrophic event. For CNN, the continuous FDIA causes a longer jump (even beyond the initial RUL value) when compared to the FDIA in LSTM and GRU. Of course, there is a higher chance that this will be flagged as a potential fault either in the engine or in the PdM system, and will cause unnecessary engine maintenance and will increase the aircraft downtown causing a financial loss to the flight operator.

In the case of piece-wise RUL prediction for engine ID 17 under interim FDIA, it is observed in Fig. 4 that the attack causes a similar jump as shown in the case of continuous FDIA in Fig. 3. However, the effect of the attack flushes away way sooner when compared to the continuous FDIA case. However, note that the attack duration was only 20 cycles, but it took more than 45 cycles to flush out the effect by the PdM system. Hence, if maintenance is due around that period, it may lead to catastrophic consequences. Once again, the piece-wise RUL prediction results indicate that employing CNN in PdM systems may result in systems that are very sensitive to the FDIA and hence special measures should be taken for designing a CNN-based PdM.

D. Impact of sequence length on resiliency of GRU

Since GRU has performed best among the DL algorithms as shown in the experimental results in the previous subsections, in Fig. 5 we compare four different GRU networks under FDI attack. The GRU networks have structures GRU1(100,100,100) lh(90), GRU2(100,100,100) lh(80), GRU3(100,100,100) lh(70), and GRU4(100,100,100) lh(60). We observe that the GRU network with architecture GRU2(100,100,100) lh 80 has the least value of true RMSE (5.36), which means that it predicts RUL quite accurately, however, it is less resilient to both continuous and interim FDIA. In contrast, GRU with network architecture GRU3(100,100,100) lh(70) shows the second-best performance in predicting the RUL (RMSE of 6.89), however, in terms of resiliency, this network is the least affected by continuous and interim FDIA. This indeed shows an interesting insight that the sequence length affects not only the accuracy but also the resiliency of the model. It also indicates that accuracy should not be the only factor while designing a PdM system. For instance, in terms of accuracy GRU2 is the typical choice. However, if both accuracy and resiliency are considered, GRU3 is can be an ideal choice (at the cost of losing some accuracy).

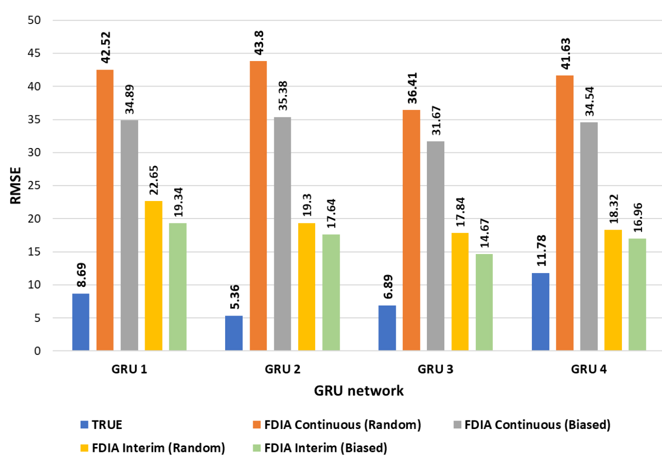

Fig. 5: RMSE comparison of different GRU networks

IV. Discussion

In this work, we first evaluate three different DL algorithms on the C-MAPSS dataset and obtained results show a great prospect for deep learning in PdM. Results show that the GRU performed 1.3-1.9 times better than the recent works that use deep learning on the C-MAPSS dataset [21], [23], [27]. The impact analysis of FDIA on aircraft sensors in the C-MAPSS dataset provides some interesting insights. We observe that CNN based PdM model is greatly affected by both random and biased FDIA. In the case of interim FDIA, CNN's random and biased RMSE are 18 and 11 times higher than the true RMSE, respectively, and in the case of continuous, the random and biased RMSE are 6 and 4 times higher than the true RMSE, respectively. We also observe that the GRU-based PdM model is more resilient to both random and biased in comparison with CNN and LSTM-based PdM models. Even though the GRU is least affected by both random and biased FDIA, their RMSE is 8 and 6 times higher than the true RMSE in the case of continuous FDIA, respectively. In the case of interim FDIA, the random and biased RMSE are 4 and 3 times higher than the true RMSE, respectively, making it disastrous for the PdM system. This may result in the delay of timely maintenance for the aircraft engine and eventually result in engine failure at some point. Note, the attack signature of FDIA is very close to the original sensor output making it harder to be detected by common defense mechanisms in an EHM system.

A piece-wise RUL predicting approach is used in visualizing the impact of attacks on the sensors, which clearly shows that the PdM system is susceptible to sensor attacks. CNN based piece-wise RUL prediction results show that special measures should be taken when designing and adopting CNN-based PdM systems (such as the cases in [32]–[35]) as they are very sensitive to the FDIA. Fig.5, gives an interesting insight into the relationship between accuracy and resiliency of the GRU network. It shows the need for considering the relationship between the accuracy, resiliency and sequence length of a DL mode (such as GRU in our case) in the design phase. Indeed, such an analysis can serve as empirical guidance to the development of subsequent data-driven PdM systems.

All of these obtained results show that DL-based PdM systems have a great prospect for aircraft maintenance, however, they are very susceptible to sensor attacks. Hence it is required to investigate proper detection techniques to detect such stealthy attacks and special care should be taken when manufacturing IoT sensors for DL/AI applications. For the same reason, while designing a PdM system, the designer also must consider the resiliency of the DL algorithm instead of just emphasizing on the algorithm's accuracy.

V. Conclusions and Future Works

This paper compares the performance of LSTM, GRU, and CNN for RUL prediction using the C-MAPSS dataset, and explores the impacts of continuous and interim FDI attacks on these deep learning algorithms. We observe that the GRU is a better suited DL technique when compared to LSTM and CNN in terms of accuracy. The obtained results show that both continuous and interim FDIA have a substantial impact on the RUL prediction even if only a few IoT sensors are attacked. We also observed that the GRU-based PdM model is more resilient to FDIA, whereas CNN is dramatically sensitive to both continuous and interim FDIA. Finally, we explored that there exists a relationship between the accuracy and sequence length in the GRU-based PdM model which can serve as empirical guidance to the development of data-driven PdM systems. In the future, we plan to develop an end-to-end methodology for the detection and mitigation of sensor attacks in a PdM system.

References

[1] R. K. Mobley, *An introduction to predictive maintenance*. Elsevier, 2002.

[2] "Predictive maintenance benefits for the freight logistics industr," Available: https://www.ibm.com/downloads/cas/AVNOLWQW.

[3] M. A. der Mauer, T. Behrens, M. Derakhshanmanesh, C. Hansen, and S. Muderack, "Applying sound-based analysis at porsche production: Towards predictive maintenance of production machines using deep learning and internet-of-things technology," in *Digitalization Cases*. Springer, 2019, pp. 79–97.

[4] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats to internet-of-things (iot) devices and applications," *arXiv preprint arXiv:1802.02041*, 2018.

[5] "Cyber-attacks On Smart Factories Are On The Rise." Available: https://smartmachinesandfactories.com/news/fullstory.php/aid/459/Cyber-attacks_on_smart_factories_are_on_the_rise.html.

[6] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE transactions on control of network systems*, vol. 1, no. 4, pp. 370–379, 2014.

[7] "The Rolls-Royce Intelligent Engine — Driven by data," Available: https://www.rolls-royce.com/media/press-releases/2018/06-02-2018-rr-intelligentengine-driven-by-data.aspx.

[8] "Predictive digonostics, Bosch," Available: https://www.bosch-mobility-solutions.com/en/products-and-services/mobility-services/predictive-diagnostics/.

[9] "Transforming Railroad Asset Management: Going Smart with Predictive Maintenance," Available: https://www.tcs.com/content/dam/tcs/pdf/Industries/travel-and-hospitality/Transforming-Railroad-Asset-Management.pdf.

[10] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2016.

[11] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system," *Journal of Parallel and Distributed Computing*, vol. 103, pp. 32–41, 2017.

[12] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 48–59, 2017.

[13] "Artificial intelligence for predictive maintenance, Aerospace Manufacturing and Design Magazine," Available: https://www.aerospacemanufacturinganddesign.com/article/artificial-intelligence-for-predictive-maintenance/.

[14] "USAF Launches Predictive Maintenance For Three Fleets," Available: https://aviationweek.com/defense/usaf-launches-predictive-maintenance-three-fleets.

[15] "The US Air Force Is Adding Algorithms to Predict When Planes Will Break, Defense One Magazine." Available: https://www.defenseone.com/business/2018/05/us-air-force-adding-algorithms-predict-when-planes-will-break/148234/.

[16] "IOT Use Cases and Innovation in IOT," Available: https://medium.com/@billsoftnet/iot-use-cases-and-innovation-in-iot-6b4e49fbc9dc.

[17] "Maintaining the data-rich Pratt Whitney GTF engine," Available: https://www.sae.org/news/2018/10/maintaining-the-data-rich-pratt--whitney-gtf-engine.

[18] Bruce Jackson, "Threat of a remote cyberattack on today's aircraft is real," 2019, [Online; accessed 01-07-2019]. [Online]. Available: https://www.darkreading.com/iot/threat-of-a-remote-cyberattack-on-todays-aircraft-is-real/a/d-id/1333551

[19] David Cenciotti, "Cybersecurity in the sky: Internet of things capabilities making aircraft more exposed to cyber threats than ever before," 2017, [Online; accessed 20-June-2017]. [Online]. Available: https://theaviationist.com/2017/06/20/cybersecurity-in-the-sky-internet-of-things-capabilities-to-make-aircraft-more-exposed-to-cyber-threats-than-ever-before/

[20] A. Saxena and K. Goebel, "C-mapss data set," *NASA Ames Prognostics Data Repository*, 2008.

[21] C. Zheng, W. Liu, B. Chen, D. Gao, Y. Cheng, Y. Yang, X. Zhang, S. Li, Z. Huang, and J. Peng, "A data-driven approach for remaining useful life prediction of aircraft engines," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*. IEEE, 2018, pp. 184–189.

[22] S. Zheng, K. Ristovski, A. Farahat, and C. Gupta, "Long short-term memory network for remaining useful life estimation," in *2017 IEEE International Conference on Prognostics and Health Management (ICPHM)*. IEEE, 2017, pp. 88–95.

[23] A. L. Ellefsen, E. Bjørlykhaug, V. Æsøy, S. Ushakov, and H. Zhang, "Remaining useful life predictions for turbofan engine degradation using semi-supervised deep architecture," *Reliability Engineering & System Safety*, vol. 183, pp. 240–251, 2019.

[24] Lee Neubecker, "Could a sonic weapon have caused the two recent boeing 737 max 8 crashes?" 2019, [Online; accessed 22-March-2019]. [Online]. Available: https://leeneubecker.com/sonic-weapon-attack-boeing/

[25] US Department of Homeland Security CISA Cyber + Infrastructure, "Can bus network implementation in avionics," 2019, [Online; accessed 13-September-2019]. [Online]. Available: https://www.us-cert.gov/ics/alerts/ics-alert-19-211-01

[26] G. R. Mode, P. Calyam, and K. A. Hoque, "False data injection attacks in internet of things and deep learning enabled predictive analytics," *arXiv preprint arXiv:1910.01716*, 2019.

[27] B. Wang, Y. Lei, N. Li, and T. Yan, "Deep separable convolutional network for remaining useful life prediction of machinery," *Mechanical Systems and Signal Processing*, vol. 134, p. 106330, 2019.

[28] F. O. Heimes, "Recurrent neural networks for remaining useful life estimation," in *2008 international conference on prognostics and health management*. IEEE, 2008, pp. 1–6.

[29] G. S. Babu, P. Zhao, and X.-L. Li, "Deep convolutional neural network based regression approach for estimation of remaining useful life," in *International conference on database systems for advanced applications*. Springer, 2016, pp. 214–228.

[30] S. Zheng, K. Ristovski, A. Farahat, and C. Gupta, "Long short-term memory network for remaining useful life estimation," in *2017 IEEE International Conference on Prognostics and Health Management (ICPHM)*. IEEE, 2017, pp. 88–95.

[31] D. K. Frederick, J. A. DeCastro, and J. S. Litt, "User's guide for the commercial modular aero-propulsion system simulation (c-mapss)," 2007.

[32] W. Silva, "Cnn-pdm: A convolutional neural network framework for assets predictive maintenance," 2019.

[33] N. Günnemann and J. Pfeffer, "Predicting defective engines using convolutional neural networks on temporal vibration signals," in *First International Workshop on Learning with Imbalanced Domains: Theory and Applications*, 2017, pp. 92–102.

[34] T. Huuhtanen and A. Jung, "Predictive maintenance of photovoltaic panels via deep learning," in *2018 IEEE Data Science Workshop (DSW)*. IEEE, 2018, pp. 66–70.

[35] R. Caponetto, F. Rizzo, L. Russotti, and M. Xibilia, "Deep learning algorithm for predictive maintenance of rotating machines through the analysis of the orbits shape of the rotor shaft," in *International Conference on Smart Innovation, Ergonomics and Applied Human Factors*. Springer, 2019, pp. 245–250.