Sensor-based Threats to Internet-of-Things and Machine Learning enabled Predictive Analytics

Gautam Raj Mode
Department of Electrical Engineering
& Computer Science
University of Missouri, Columbia,
MO, USA
gmwyc@mail.missouri.edu

Prasad Calyam
Department of Electrical Engineering
& Computer Science
University of Missouri, Columbia,
MO, USA
calyamp@missouri.edu

Khaza Anuarul Hoque
Department of Electrical Engineering
& Computer Science
University of Missouri, Columbia,
MO, USA
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 in predicting faults in a component or system powered by state-of-the-art machine learning (ML) algorithms and the Internet Internet-of-Things (IoT) sensors. However, IoT sensors and ML algorithms, both are known for their vulnerabilities to attacks. In this work, we consider an aircraft PdM system for detection of future defects in an aircraft engine by predicting the engine's Remaining Useful Life (RUL). We compare between Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Convolutional Neural Network (CNN) in predicting RUL and utilize GRU for RUL prediction of an aircraft engine as it showed greater accuracy compared to others. Afterward, we apply the false data injection attack (FDIA) and denial of service (DoS) attacks on aircraft engine sensor data and evaluate their impact on the GRU-based RUL prediction. Our experimental results demonstrate that the attacks on IoT sensors strongly defects the RUL prediction.

KEYWORDS

Predictive Maintenance, Machine learning, LSTM, GRU, CNN, remaining useful life, denial-of-service attack, false-data injection attack

ACM Reference format:
Gautam Raj Mode, Prasad Calyam, and Khaza Anuarul Hoque. 2019. Sensor-based Threats to Internet-of-Things and Machine Learning enabled Predictive Analytics. In *Proceedings of The 17th ACM Conference on Embedded Networked Sensor Systems, New York, USA, November 10–13 2019 (AIChallengeIoT'19),* 7 pages.
https://doi.org/00.0001

1 INTRODUCTION

In the recent years, the field of Artificial Intelligence (AI) and Machine Learning (ML) has seen exponential growth followed by a huge demand in the industry. Due to their immense demand, they find their applications in mobile vision [17], healthcare [26], face detection [23], fault detection [20], and many others, but there are leading concerns on effect of attacks on AI and ML. Adversarial ML [18, 22, 40] is technique employed by the attacker to intentionally make the ML to make a wrong classification or a wrong prediction. The attacker can either attack the ML pipeline or the data that is used for training and testing ML. In order to show the effect of attacks on ML, we have performed a case study on aircraft Predictive Maintenance (PdM) that employs ML algorithms.

Nowadays, due to the rapid development in the field of avionics, the aircraft engines have become increasingly sophisticated and complex, which means unexpected faults could result in consequences that range from flight delays to an accident that may cost millions to the airline, but most importantly loss of lives. Recently, predictive maintenance (PdM) [10, 31, 42] has been recognized as a better-suited strategy for aircraft engines as it considers wear and tear of the equipment, and most importantly it depends on the data from the equipment, removing the need for periodical checks [27].

As an ideal maintenance policy, PdM collects different parameters from an aircraft engine, detects minuscule changes in the functioning of an engine, and discovers faults, including when, where, and which type of failure that may occur by using machine learning algorithms [11]. With the fault information, PdM could arrange appropriate maintenance requests to the engine manufacturer even before the fault is encountered. To design the best-suited PdM for an aircraft, a comprehensive understanding of Engine Health Monitoring (EHM) [19] systems is required. Figure 1 shows a generic EHM architecture. An EHM system has several IoT (Internet of Things) sensors connected to wireless network, which monitor different parameters of an aircraft engine, and sends out alerts to the engine manufacturer if the Remaining Useful Life (RUL) [32] of the engine is approaching its end of life. [1] An EHM system employs PdM systems to predict the RUL using the data collected from the IoT sensors. Unfortunately, IoT sensors are susceptible to attacks [33], which possess a significant threat for the overall PdM system. Attacking the IoT sensors would result in sending faulty data to the ML algorithm for prediction, which will eventually result in incorrect RUL predictions. This may result in delay of timely maintenance and lead to mid-air engine failures which is catastrophic.

An aircraft in general has several avionic systems. The systems include ground proximity warning system [12], traffic alert and

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

AIChallengeIoT'19, November 10–13 2019, New York, USA
© 2019 Association for Computing Machinery.
ACM ISBN 12343…$15.00
https://doi.org/00.0001

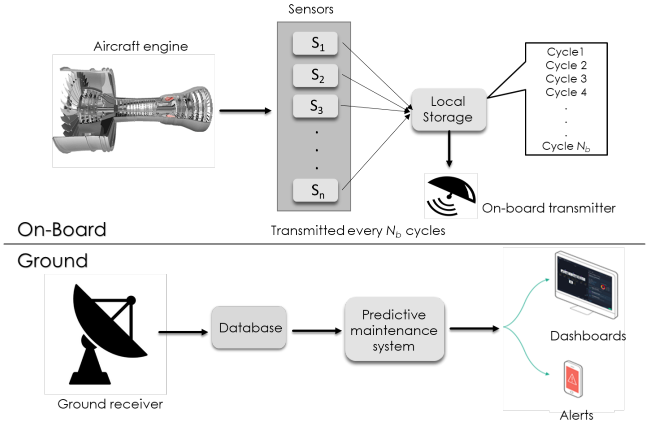


Figure 1: Engine health monitoring (EHM) system architecture

collision avoidance system [21], instrument landing system [25], etc . Each system has several avionic sensors that collect and feed different parameters that makes these systems functional. An attack on these systems may lead to deadly consequences. Even though the concept of attacks on these system seems a distant concept, but there are many works [14, 28, 29, 35] that talk otherwise.

In this paper, we investigate the effects of attacks on IoT sensors in a PdM system that relies on a machine learning algorithm. We compare between Long Short-Term Memory (LSTM), Gated recurrent unit (GRU), and Convolutional neural network (CNN) in order to select accurate predictor for PdM. We perform the False Data Injection Attack (FDIA) and Denial of Service (DoS) attacks on different engine sensors in the C-MAPSS [30] (Commercial Modular Aero-Propulsion System Simulation) data set [2]. We evaluate these attacks on an attack scenario, analyze and measure their impacts on the RUL prediction. The FDIA attack mentioned in this paper is harder to detect even with common defense mechanisms in place. To the best of our knowledge, this is the first work that demonstrates the effects of attacks on IoT sensors in a PdM system.

The rest of the paper is organized as follows. Section II briefly discusses the Engine Health Monitoring (EHM) systems and Predictive Maintenance (PdM). Section III introduces LSTM, GRU, CNN, and the NASA C-MAPSS data set used for our experiment. In Section IV, we present an attack scenario on the RUL prediction. Experiment results of those attack are described in Section V. Section VI presents the observations from those obtained results, and Section VII concludes the paper.

2 PRELIMINARIES

2.1 Engine health monitoring (EHM) system

An aircraft engine is a complex system, so it requires adequate monitoring to ensure safe operation and in-time maintenance [19]. Several displays and dials in the cockpit give different measurements like exhaust gas temperatures, engine pressure ratio, the pressure at fan inlet, rotational speeds, etc. All these parameters are crucial in indicating the health of the engine; they serve as early indicators of failure and prevent costly component damage.

In order to accomplish the task of monitoring several parameters in an engine, Engine health monitoring (EHM) systems [39] have been in service for three decades. In an EHM system, IoT sensors are mounted inside and outside of an engine to monitor different parameters. All the IoT sensors are connected to a wireless network [3], which uses radio frequency for transmitting sensor output to central engine control [3]. Figure 1 shows a general EHM architecture. The sensors onboard the engine send time series data (cycles) every hour to the local storage onboard the airplane. After every N_b cycles of data are captured, the data is transmitted to the ground station. At the ground station, the incoming live data is stored in the database and sent to PdM system to predict RUL of the engine. The PdM system sends out alerts if the predicted RUL is less than the permissible safe operation RUL of the engine.

2.2 Predictive maintenance (PdM)

In manufacturing supply chains, unexpected failures are considered as primary operational risk as it can hinder productivity and can incur huge losses. For example, in modern automotive industry, an assembly line has several robots working on a car, and even if one of the robots fails, it will result in the total halt of the assembly line, causing loss of valuable production time and money. To overcome this problem, PdM strategies are employed. PdM is an industry 4.0 solution, which assists in predicting the future state of physical assets. It helps in better-informed maintenance decisions, to prevent unexpected delays.

PdM systems are employed in major industries like Nuclear power plants, aviation industry, automotive industry, and health care services. PdM allows for convenient scheduling of corrective maintenance parts for the equipment can be ordered beforehand to avoid last minute hassle, which saves a lot of valuable production time. PdM is well suited for making an informed decision when dealing with time-series data. A data-driven based model of PdM employ some the remarkable strategies like Random Forest algorithm [41], Artificial Neural Networks (ANN) [4], fuzzy models [34], Big data frameworks [6]. In this paper, an LSTM based deep learning approach is employed in predicting RUL of an aircraft engine.

3 ML ALGORITHMS FOR RUL PREDICTION

In this section, the LSTM, GRU and CNN networks for RUL prediction are presented, including the architecture of the network, the NASA C-MAPSS data set, and feature extraction from the data set.

3.1 Long short-term memory model (LSTM)

Long Short-Term Memory Network [16] is a special kind of Recursive Neural Network (RNN), capable of learning long-term dependencies. LSTM is explicitly designed to avoid long term dependency problem, which is prevalent is RNN. It has achieved great praise in the field of machine learning and speech recognition. Some the neural networks have a dependency problem, but an LSTM can overcome the problem of dependency by controlling the flow of information using input, output and forget gate. The input gate controls the flow of input activation into the memory cell. The

[2] a popular turbofan engine degradation data set published by NASA's Prognostics Center of Excellence (PCoE)

output gate controls the output flow of cell activation into the rest of the network.

Construction of LSTM and its network design have been extensively talked in extended paper cite paper.

3.2 Gated recurrent unit (GRU)

The GRU was proposed by Cho et al. [8]. It operates using reset gate and update gates. GRUs are improved version of standard recurrent neural network. Similar to the LSTM unit, the GRU has gating units that modulate the flow of information, however, without having a separate memory cells. GRU's performance on certain tasks of polyphonic music modeling and speech signal modeling was found to be similar to that of LSTM. GRUs have been shown to exhibit even better performance on certain smaller datasets [45].

Construction of GRU and its network design have been extensively talked [9].

3.3 Convolutional neural network (CNN)

A Convolutional Neural Network (ConvNet/CNN) is a Deep Learning algorithm. In recent years, the CNN has achieved exceptional success in various research fields [5] because it has many advantages over traditional machine learning approaches such as MLP [37]. CNN find their applications in mobile vision [17], healthcare [26], face detection [23], fault detection [20], and many others. A 1D CNN model is utilized in this paper to estimate the RUL of the engine.

Construction of CNN and its network design have been extensively talked [20].

3.4 C-MAPSS data set

To evaluate the performance of the proposed LSTM network, we use a well-known dataset, NASA's turbofan engine degradation simulation dataset C-MAPSS (Commercial Modular Aero-Propulsion System Simulation). This dataset includes 21 sensor data with a different number of operating conditions and fault conditions. In this dataset, there are four sub-datasets (FD001-04) with various operating conditions and fault conditions. Every subset has training data and test data. The test data has run to failure data from several engines of the same type. Each row in test data is a time cycle which can be defined as an hour of operation. A time cycle has 26 columns where the 1st column represents engine ID, and the 2nd column represents the current operational cycle number. The columns from 3 to 5 represent the three operational settings and columns from 6-26 represent the 21 sensor values.[3].

The time series data stops only when a fault is encountered. For example, an engine with ID 1 has 192 time cycles of data, which means the engine has developed a fault at the 192nd time cycle. The test data contains data only for some time cycles as our goal is to estimate the remaining operational time cycles before failure based on a given incomplete data.

3.5 Evaluation metric

To evaluate the performance of the predictors on the test data, we utilize the mean absolute error (MAE) metric. MAE is widely used as an evaluation metric in model evaluation studies. MAE measures the average magnitude of the errors in a set of predictions, without considering their direction. Hence, MAE can be considered as a more natural measure of average error in many cases when compared to the Root Mean Square Error (RMSE) metric [7, 43]. MAE gives equal penalty weights to the model when the estimated RUL is either larger or smaller than the true RUL.

4 ATTACKS ON A PdM SYSTEM

In this paper, we consider performing False Data Injection Attack (FDIA) and Denial of Service (DoS) attacks on the PdM system.

4.1 False data injection attack (FDIA)

False Data Injection Attack (FDIA) [24] is capable of disrupting the RUL prediction process in a PdM system. A successful FDIA can cause the engine sensors to output erroneous values to the central engine control, and thus make either physical or economic impact on the predictive maintenance model. 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 Equation (1).

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

For an effective FDIA vector formulation, the adversary needs to have knowledge of the communication topology used by the sensors to communicate with central engine control, have physical access to the sensors, know whereabouts of the airplane and its maintenance history. An FDIA attack can be *constrained* and *unconstrained*, which are further defined as follows:

1) *Constrained*: The attacker has access to a limited number of sensors, and some part of the communication network.
2) *Unconstrained*: The attacker has access to all of the sensors and also has total control of the communication network.

In this paper constrained attacks are considered. In one the works, it is shown that false data injection can be done using spoofing techniques. Tippenhauer et al. [38] showed a spoof attack scenario on GPS-enabled devices. In this attack scenario, a forged GPS signal is transmitted to the device to alter the location. In this way real location of the device is disguised and attacker can perform physical attack on the device. In an another work by Giannetos et al. [13] introduced an app named Spy-sense, which monitors behaviours of several sensors in a device. The app can manipulate sensor data by deleting or modifying it. Spy-sense exploits active memory region in a device and relays sensitive data covertly. All these works show that FDIA attack can be performed by even without gaining direct access to the system.

4.2 Denial of service attack (DoS)

Denial of service attack (DoS) [44], also known as interruption attacks. It can partially or entirely disrupt the data exchange between

[3] More details about these 21 sensors can be found in cite paper

sensors and central engine control. In this paper, we consider a DoS attack that entirely disrupts the communication between sensors and central engine control for a period of T. For instance, if x_i is the original sensor output of i^{th} sensor, and d_i is the attacked senor output of i^{th} sensor for the attack period from T_{start} to T_{end}, then the DoS attack is formulated as follows:

$$d_i = \begin{cases} 0 & T_{start} < T < T_{end} \\ x_i & else \end{cases} \tag{2}$$

Note that, for a DoS attack to be effective, the intruder needs to know the communication topology used by the IoT sensors, have physical access to the sensors, know the whereabouts of the airplane. In this paper, *constrained* DoS attacks are considered. The properties of constrained attacks are similar to those mentioned in the FDIA attack.

Some works have shown that DoS attack can be implemented even without a connected network. Son *et al.* [36] showed that it is possible to obstruct the flight control of a drone by exploiting gyroscope using a sound signal. It showed that the gyroscope can be exploited by an audio signal matching the resonant frequency of the gyroscope. In doing so the attacker can change the course or even shutdown the drone. Recently, ICS-CERT published an alert on a list of accelerometers used in IoT devices which can be exploited using vibrational force [1]. All these works show that to perform DoS attack can be performed without gaining direct access to the system.

4.3 Attack scenario

As shown in Figure 1 of the 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 send 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.

In a more practical sense, the degradation of the engine is very negligible at the beginning, but as time proceeds, the degradation follows a linear trend, and it increases as the engine approaches the end of life. 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 data set is taken, it is found to be N^d_{avg}. An adversary having the knowledge of N^d_{avg} can perform the attacks after the degradation initiates, making the attack more destructive. To study the impact of two different attacks on PdM systems, we consider an attack scenario.

In the attack scenario, the attackers are on-board the airplane. They can perform FDIA attack by using spoofing techniques [38] as mentioned previously in section 4.1. In the case of DoS attack the attackers can attack the sensors without gaining direct access to the system by using techniques [1, 36] mentioned in section 4.2. To perform an effective attack, the adversary have knowledge of the aircraft's flight hours after maintenance. An attacker who has knowledge of N^d_{avg} can perform the attacks after the degradation initiates, making the attack more destructive in nature.

5 EXPERIMENTAL RESULTS

Section 5.1 compares different predictors. In Section 5.2, the impact of attacks on the PdM system has been presented, which includes the study of different attack signatures, impact of attacks on the RUL prediction, and piece-wise RUL prediction.

5.1 Comparison of predictors

In order to select the best predictor for the PdM, we compare three different ML algorithms for the C-MAPSS data set. Table 1 represents the comparison between predictors with architectures LSTM(100,100,100), lh(80), GRU(100,100,100), lh(80) and CNN(64,64,64), lh(100). The notation LSTM(100,100,100) lh(80) refers to network that has 100 nodes in the hidden layers of the first LSTM layer, 100 nodes in the hidden layers of the second LSTM layer, 100 nodes in the hidden layers of the third LSTM layer, and a sequence length of 80. At the end, there is a 1-dimensional output layer.

Table 1: MAE comparison for different predictors

Predictor architecture	FD001
	MAE
LSTM(100,100,100), lh(80)	7.26
GRU(100,100,100), lh(80)	4.64
CNN(64,64,64), lh(100)	8.21

From Table 1 it is evident that the predictor GRU(100, 100, 100) with a sequence length equal to 80 has the least MAE of 4.64. It means that GRU is very efficient in predicting accurate RUL for this dataset. Hence, we choose this predictor for modeling the attacks on the PdM system. It can be observed that both the sequence length and the number of layers are important parameters in achieving accurate RUL.

5.2 Attacks on the PdM system

In this section, the impact of different attacks on RUL prediction of the GRU network has been presented.

Attack model setup

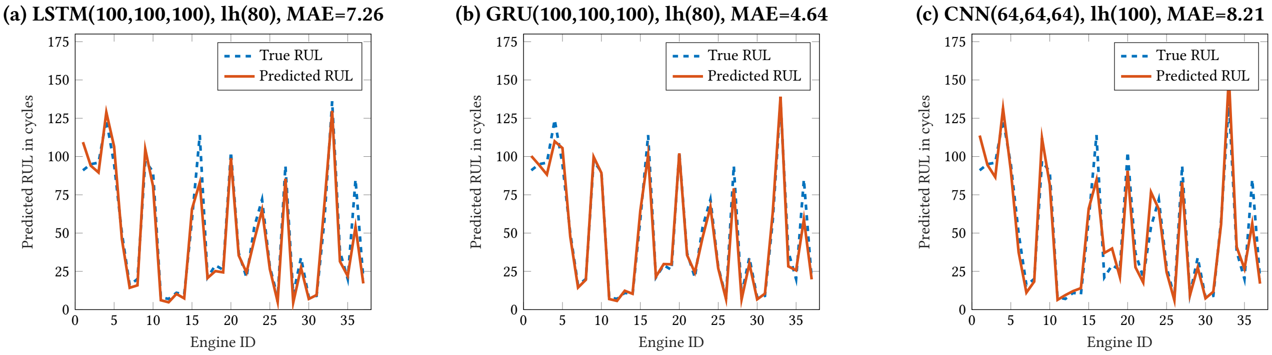
The average degradation point of the engine N^d_{avg} is considered as 130 for the FD001 data set [15] [2] [46], and aircraft sends 20 time cycles (N_b) of data to the ground at a time. In the attack scenario, the attacker has initiated the attacks after N^d_{avg}, which is 130 time cycles, and the attack duration is 20 hours, which is 20 time cycles.

In train and test data set, 7 out of 21 sensors can be ignored as their values after normalization remain constant. Adversarial attacks can be performed on the remaining 14 sensors.

Attack signatures

In this section, we present the attack signatures of FDIA and DoS attacks as described in the section 4.

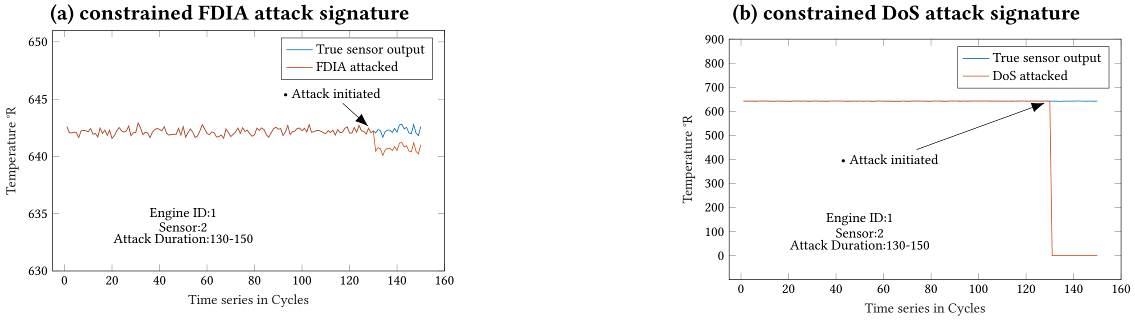
FDIA: To model the FDIA attack on sensors, we add a vicious vector to the original vector modifies the sensor output by a very small margin (0.2% to 0.3%). Figure 3(a) shows the comparison between the original and FDIA attacked output signal of sensor 2 for engine ID 3 for constrained attacks, and it is described as follows.


(a) LSTM(100,100,100), lh(80), MAE=7.26

(b) GRU(100,100,100), lh(80), MAE=4.64

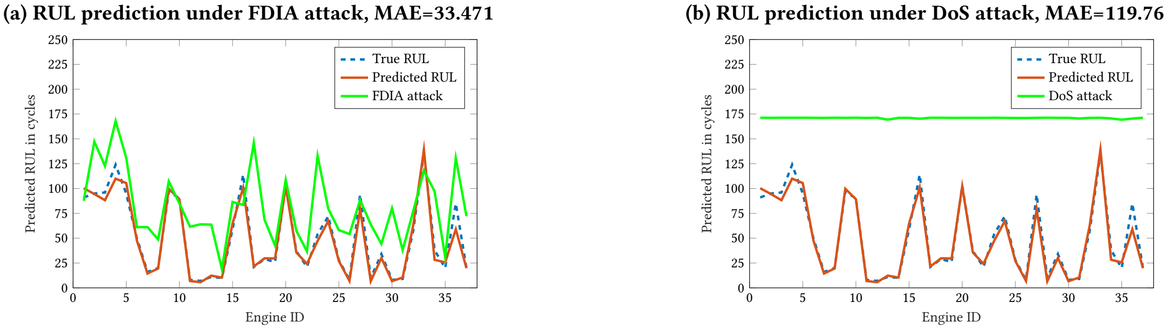
(c) CNN(64,64,64), lh(100), MAE=8.21

Figure 2: Comparison of ML algorithms


(a) constrained FDIA attack signature

(b) constrained DoS attack signature

Figure 3: Attack signatures


(a) RUL prediction under FDIA attack, MAE=33.471

(b) RUL prediction under DoS attack, MAE=119.76

Figure 4: Attack scenario

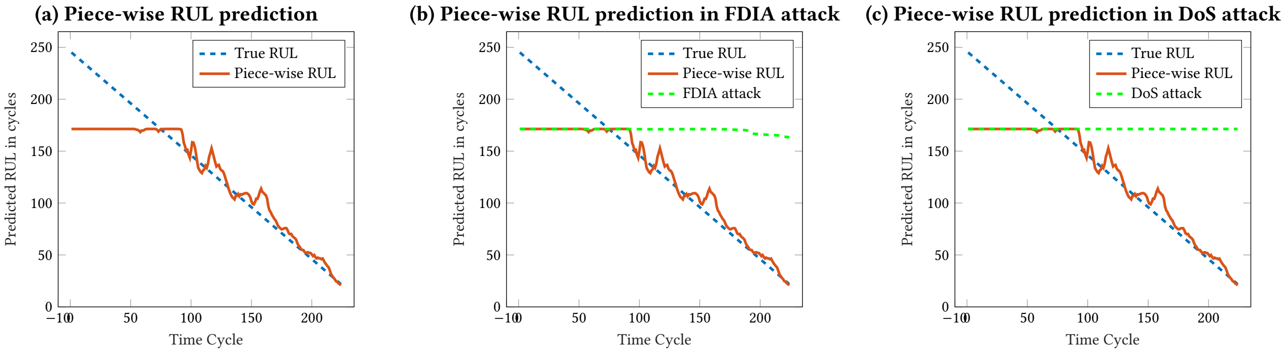
Constrained: In this attack, the sensor output from time cycles 130 to 150 are attacked. As shown in Figure 3(a), the attack signature is also very similar to the original signal, making it stealthy and harder to detect even with common defense mechanisms in place. Note, in the constrained attack the adversary has limited access to sensors, but he can increase the duration of the attack by taking multiple flights.

DoS attack: As the communication network is attacked using a DoS attack, the data packets are dropped, making the sensor output to zero. Figure 3(b) represents the comparison between the original and DoS attacked output of sensor 2 for engine ID 3. The properties of constrained attack are similar to those mentioned in the FDIA attack.

One can argue that an attacker attacking the sensors can directly mislead the avionic systems, but the main goal of these attack is to show the effect of attacks on data provided to ML.

Impact analysis of different attacks on the aircraft PdM system

To show the impact of FDIA and DoS attacks on the aircraft PdM system, we implement attacks for scenario mentioned previously in Section 4.3. To make the attack more practical 3 sensors are attacked for DoS and 7 for FDIA.



(a) Piece-wise RUL prediction (b) Piece-wise RUL prediction in FDIA attack (c) Piece-wise RUL prediction in DoS attack

Figure 5: Piece-wise RUL prediction

In this scenario, the adversary performs attacks between 130 and 150 time cycles. The attacker has limited access to the sensors in the engine. Figures 4(a) and 4(b) represents the effected RUL prediction for two different attacks. In order to make this scenario more effective, the adversary may have to take multiple flights to attacks more time cycles of data.

Piece-wise RUL prediction

The attacks evaluated in the scenario take into account the attacks performed on all of the engine data in the C-MAPSS test data set. To show the impact of 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.

Figure 5(a) shows an example of an engine data from the data set 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 Figure 5(a), it is evident that as the time series approaches the end of life, the predicted RUL is close to the true RUL, because the GRU model has more time series data to accurately predict the RUL. Figure 5(b) and 5(c) shows two different attacks on the aircraft PdM system. The attacks are performed on an engine with 242 time cycles of test data.

Table 2: MAE comparison for the attack scenario

Scenario	MAE		
	True	FDIA	DoS
1	4.64	33.471	119.76

For FDIA and DoS attacks shown in Figure 5(b) and Figure 5(c), we observe that the predicted RUL during the attack remains constant at 170 for the attack duration which clearly shows that PdM system are susceptible to adversarial threats.

6 DISCUSSION

In this work, we first evaluate different predictors on C-MAPSS dataset, and obtained results show a great prospect for deep learning in PdM. It is observed that sequence length and network architecture are crucial in predicting accurate RUL.

The impact analysis of different attacks on aircraft sensors in the C-MAPSS dataset provides some interesting insights. In the case of FDIA attack, we observe that the constrained attacks have great impact on the PdM system. In the event of DoS attack, constrained attack was proved to be fatal to the PdM system. Note that 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.

Table 2 shows the outcome of different attacks on the GRU network. In the table, the *True* column represents MAE of the GRU architecture without any attack, and the rest of the columns are MAE of the network after different attacks. It can be observed that DoS attack has a significant impact on the PdM system, with MAE of 119. Whereas FDIA attack has a minimal impact (MAE of 33.471). Note, even though the impact is minimum, the MAE is 7 times greater than the true MAE (4.64), making it disastrous for the PdM system. This may result in delay of timely maintenance for the aircraft engine and eventually result in engine failure at some point which is disastrous.

All of these obtained results show that machine learning-based PdM systems have a great prospect for aircraft maintenance. However, our results indicate that they are very susceptible to attacks. The need of engineering defense mechanisms that detect even the stealthiest attacks, and developing IoT sensors that are resilient to physical attacks is very much needed. Hence, while designing PdM systems, the designer must consider incorporating the ability to make the systems less vulnerable and more resilient to different kinds of attacks, such as those investigated in this paper.

7 CONCLUSIONS AND FUTURE WORKS

This paper compares different predictors for estimation of RUL for C-MAPSS dataset, and explores the impacts of attacks on such predictors. We model two different attacks (DoS and FDIA attack) on the IoT sensors that provide data to PdM system and evaluate their impacts on RUL prediction. The obtained results show that DoS attack is the most lethal attack for the aircraft PdM system. Besides, the FDIA also has a substantial impact on the RUL prediction. In the future, we plan to develop an end-to-end methodology for detecting and mitigating attacks in a PdM system.

REFERENCES

[1] [n. d.]. Mems accelerometer hardware design flaws (update a). https://www.us-cert.gov/ics/alerts/ICS-ALERT-17-073-01A. ([n. d.]). Accessed: 2017-05-30.

[2] Giduthuri Sateesh Babu, Peilin Zhao, and Xiao-Li Li. 2016. Deep convolutional neural network based regression approach for estimation of remaining useful life. In *International conference on database systems for advanced applications*. Springer, 214–228.

[3] Haowei Bai, Mohammed Atiquzzaman, and David Lilja. 2004. Wireless sensor network for aircraft health monitoring. In *First International Conference on Broadband Networks*. IEEE, 748–750.

[4] Pramod Bangalore and Lina Bertling Tjernberg. 2013. An approach for self evolving neural network based algorithm for fault prognosis in wind turbine. In *2013 IEEE Grenoble Conference*. IEEE, 1–6.

[5] Ashwin Bhandare, Maithili Bhide, Pranav Gokhale, and Rohan Chandavarkar. 2016. Applications of convolutional neural networks. *International Journal of Computer Science and Information Technologies* 7, 5 (2016), 2206–2215.

[6] Mikel Canizo, Enrique Onieva, Angel Conde, Santiago Charramendieta, and Salvador Trujillo. 2017. Real-time predictive maintenance for wind turbines using Big Data frameworks. In *2017 IEEE International Conference on Prognostics and Health Management (ICPHM)*. IEEE, 70–77.

[7] Tianfeng Chai and Roland R Draxler. 2014. Root mean square error (RMSE) or mean absolute error (MAE)? *Geoscientific Model Development Discussions* 7 (2014), 1525–1534.

[8] Kyunghyun Cho, Bart Van Merriënboer, Dzmitry Bahdanau, and Yoshua Bengio. 2014. On the properties of neural machine translation: Encoder-decoder approaches. *arXiv preprint arXiv:1409.1259* (2014).

[9] Junyoung Chung, Caglar Gulcehre, Kyunghyun Cho, and Yoshua Bengio. 2015. Gated feedback recurrent neural networks. In *International Conference on Machine Learning*. 2067–2075.

[10] Federico Civerchia, Stefano Bocchino, Claudio Salvadori, Enrico Rossi, Luca Maggiani, and Matteo Petracca. 2017. Industrial Internet of Things monitoring solution for advanced predictive maintenance applications. *Journal of Industrial Information Integration* 7 (2017), 4–12.

[11] Matthias Auf der Mauer, Tristan Behrens, Mahdi Derakhshanmanesh, Christopher Hansen, and Stefan Muderack. 2019. 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, 79–97.

[12] Umut Durak, David Müller, Jürgen Becker, Nikolaos S Voros, Panayiotis Alefragis, Timo Stripf, Pierre-Aimé Agnel, Gerard Rauwerda, and Kim Sunesen. 2016. Model-based development of Enhanced Ground Proximity Warning System for heterogeneous multi-core architectures. In *2016 AIAA Modeling and Simulation Technologies Conference*.

[13] Thanassis Giannetsos and Tassos Dimitriou. 2013. Spy-Sense: spyware tool for executing stealthy exploits against sensor networks. In *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy*. ACM, 7–12.

[14] Jon C Haass, J Philip Craiger, and Gary C Kessler. 2018. A Framework for Aviation Cybersecurity. In *NAECON 2018-IEEE National Aerospace and Electronics Conference*. IEEE, 132–136.

[15] Felix O Heimes. 2008. Recurrent neural networks for remaining useful life estimation. In *2008 international conference on prognostics and health management*. IEEE, 1–6.

[16] Sepp Hochreiter and Jürgen Schmidhuber. 1997. Long short-term memory. *Neural computation* 9, 8 (1997), 1735–1780.

[17] Andrew G Howard, Menglong Zhu, Bo Chen, Dmitry Kalenichenko, Weijun Wang, Tobias Weyand, Marco Andreetto, and Hartwig Adam. 2017. Mobilenets: Efficient convolutional neural networks for mobile vision applications. *arXiv preprint arXiv:1704.04861* (2017).

[18] Ling Huang, Anthony D Joseph, Blaine Nelson, Benjamin IP Rubinstein, and JD Tygar. 2011. Adversarial machine learning. In *Proceedings of the 4th ACM workshop on Security and artificial intelligence*. ACM, 43–58.

[19] Klaus Hünecke. 1997. *Jet engines: Fundamentals of theory, design and operation*. Number BOOK. Airlife.

[20] Turker Ince, Serkan Kiranyaz, Levent Eren, Murat Askar, and Moncef Gabbouj. 2016. Real-time motor fault detection by 1-D convolutional neural networks. *IEEE Transactions on Industrial Electronics* 63, 11 (2016), 7067–7075.

[21] JE Kuchar and Ann C Drumm. 2007. The traffic alert and collision avoidance system. *Lincoln Laboratory Journal* 16, 2 (2007), 277.

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

[23] Haoxiang Li, Zhe Lin, Xiaohui Shen, Jonathan Brandt, and Gang Hua. 2015. A convolutional neural network cascade for face detection. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 5325–5334.

[24] Kebina Manandhar, Xiaojun Cao, Fei Hu, and Yao Liu. 2014. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE transactions on control of network systems* 1, 4 (2014), 370–379.

[25] Jerzy Merkisz, Marta Galant, and Michał Bieda. 2017. Analysis of operating instrument landing system accuracy under simulated conditions. *Zeszyty Naukowe. Transport/Politechnika Śląska* (2017).

[26] Fausto Milletari, Nassir Navab, and Seyed-Ahmad Ahmadi. 2016. V-net: Fully convolutional neural networks for volumetric medical image segmentation. In *2016 Fourth International Conference on 3D Vision (3DV)*. IEEE, 565–571.

[27] Toshio Nakagawa. 1984. Periodic inspection policy with preventive maintenance. *Naval Research Logistics Quarterly* 31, 1 (1984), 33–40.

[28] Luke Ryon and Greg Rice. 2018. A Safety-focused Security Risk Assessment of Commercial Aircraft Avionics. In *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*. IEEE, 1–8.

[29] Krishna Sampigethaya and Radha Poovendran. 2013. Aviation cyber–physical systems: Foundations for future aircraft and air transport. *Proc. IEEE* 101, 8 (2013), 1834–1855.

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

[31] Sule Selcuk. 2017. Predictive maintenance, its implementation and latest trends. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture* 231, 9 (2017), 1670–1679.

[32] Xiao-Sheng Si, Wenbin Wang, Chang-Hua Hu, and Dong-Hua Zhou. 2011. Remaining useful life estimation–a review on the statistical data driven approaches. *European journal of operational research* 213, 1 (2011), 1–14.

[33] Amit Kumar Sikder, Giuseppe Petracca, Hidayet Aksu, Trent Jaeger, and A Selcuk Uluagac. 2018. A survey on sensor-based threats to internet-of-things (iot) devices and applications. *arXiv preprint arXiv:1802.02041* (2018).

[34] Silvio Simani, Saverio Farsoni, and Paolo Castaldi. 2014. Fault tolerant control of an offshore wind turbine model via identified fuzzy prototypes. In *2014 UKACC International Conference on Control (CONTROL)*. IEEE, 486–491.

[35] Matthew Smith, Martin Strohmeier, Jon Harman, Vincent Lenders, and Ivan Martinovic. 2019. Safety vs. Security: Attacking Avionic Systems with Humans in the Loop. *arXiv preprint arXiv:1905.08039* (2019).

[36] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. 2015. Rocking drones with intentional sound noise on gyroscopic sensors. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*. 881–896.

[37] Rakesh Ranjan Swain and Pabitra Mohan Khilar. 2016. A fuzzy MLP approach for fault diagnosis in wireless sensor networks. In *2016 IEEE region 10 conference (TENCON)*. IEEE, 3183–3188.

[38] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. 2011. On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 75–86.

[39] Irem Tumer and Anupa Bajwa. 1999. A survey of aircraft engine health monitoring systems. In *35th Joint Propulsion Conference and Exhibit*. 2528.

[40] JD Tygar. 2011. Adversarial machine learning. *IEEE Internet Computing* 15, 5 (2011), 4–6.

[41] Anoop Prakash Verma. 2012. Performance monitoring of wind turbines: a data-mining approach. (2012).

[42] Yupeng Wei, Dazhong Wu, and Janis Terpenny. 2018. Predictive maintenance for aircraft engines using data fusion. In *2018 Institute of Industrial and Systems Engineers Annual Conference and Expo, IISE 2018*.

[43] Cort J Willmott and Kenji Matsuura. 2005. Advantages of the mean absolute error (MAE) over the root mean square error (RMSE) in assessing average model performance. *Climate research* 30, 1 (2005), 79–82.

[44] Ping Yi, Ting Zhu, Qingquan Zhang, Yue Wu, and Li Pan. 2016. Puppet attack: A denial of service attack in advanced metering infrastructure network. *Journal of Network and Computer Applications* 59 (2016), 325–332.

[45] Rui Zhao, Dongzhe Wang, Ruqiang Yan, Kezhi Mao, Fei Shen, and Jinjiang Wang. 2017. Machine health monitoring using local feature-based gated recurrent unit networks. *IEEE Transactions on Industrial Electronics* 65, 2 (2017), 1539–1548.

[46] Shuai Zheng, Kosta Ristovski, Ahmed Farahat, and Chetan Gupta. 2017. Long short-term memory network for remaining useful life estimation. In *2017 IEEE International Conference on Prognostics and Health Management (ICPHM)*. IEEE, 88–95.