

# Identificazione di Anomalie su Big Data del settore Automotive

Alfredo Lubrano<sup>1</sup>, Claudio Lucchese<sup>2</sup>, Franco Maria Nardini<sup>3</sup>, Walter Negro<sup>1</sup>,  
Andrea Passarella<sup>3</sup>, Raffaele Perego<sup>3</sup>, Lorenzo Valerio<sup>3</sup>, Rossano Venturini<sup>4</sup>,

<sup>1</sup>FCA, Orbassano, Torino. <sup>2</sup>Università di Venezia. <sup>3</sup>CNR, Pisa. <sup>4</sup>Università di Pisa.

## Abstract

Lo sviluppo di nuovi prodotti caratterizzati da elevata complessità tecnologica e produttiva segue sempre di più un approccio “data-driven”, guidato dalla trasformazione in cui Big Data e tecnologie ad essi collegate giocano un ruolo centrale. In questo articolo presentiamo l’applicazione di tecniche di intelligenza artificiale (AI) a Big Data provenienti dal settore automotive. In particolare, descriviamo l’utilizzo di tecniche di Deep Learning (DL) per la ricerca di anomalie nei dati trasmessi da sensori e dispositivi di bordo che equipaggiano le moderne autovetture FCA. I risultati dimostrano che le tecniche di DL testate forniscono un ottimo strumento a supporto dei progettisti.

## 1 Introduzione

Il settore automotive sta vivendo una importante trasformazione che coinvolge tutte le fasi legate alla progettazione e alla produzione di autoveicoli. I Big Data e le tecnologie a loro connesse sono uno degli ingredienti principali di questa trasformazione che vede le principali case automobilistiche adottare oggi un approccio totalmente “data-driven” alla progettazione e produzione dei loro prodotti. Un esempio interessante di questa trasformazione riguarda la fase di testing dei nuovi modelli prodotti. Ogni nuovo modello di autovettura necessita infatti di test funzionali approfonditi realizzati mediante una flotta di prototipi instrumentati guidata in condizioni stradali e climatiche “estreme” da collaudatori professionisti. Tali collaudatori hanno il compito di sottoporre a stress le autovetture annotando e riportando agli ingegneri eventuali comportamenti anomali riscontrati a bordo. Durante questi test la sofisticata elettronica di bordo, che controlla oggi tutti i sottosistemi di cui la vettura è composta: motore, sospensioni, freni, trasmissione, ecc., raccoglie in tempo reale e memorizza i parametri di funzionamento dei singoli componenti e dispositivi. Questa ricchezza di dati permette una identificazione di anomalie molto più accurata e precisa di quella fatta in passato. Attraverso le conoscenze e l’esperienza maturata nel dominio, un esperto analizza ed interpreta i dati alla ricerca delle cause delle eventuali anomalie nel veicolo. D’altro canto, i sensori a bordo contribuiscono alla raccolta di una grandissima mole di dati - gigabytes

per ogni vettura, ogni giorno - che rende l’analisi dell’esperto onerosa in tempo e sensibile ad errori. Si rende quindi necessario automatizzare la ricerca di anomalie nei dati raccolti a supporto dell’esperto di dominio.

L’identificazione di anomalie (*Anomaly Detection*, AD) è una linea di ricerca ben definita riferita all’identificazione di oggetti, eventi oppure osservazioni che non seguono il “normale” comportamento del sistema in analisi. L’AD consente quindi di identificare pattern inusuali nei dati. Lo stato dell’arte relativo all’AD può essere raggruppato in quattro grandi famiglie di tecniche: i) statistiche, ii) spettrali, iii) information theory, iv) machine learning. Mentre le prime tre studiano le proprietà dei dati evidenziandone caratteristiche statistiche specifiche che poi vengono utilizzate successivamente per l’identificazione degli *outliers*, la quarta utilizza tecniche “supervised” proprie del machine learning per derivare predittori che, apprendendo il comportamento “normale” del sistema, sono in grado di individuare anomalie sulla base dell’errore commesso dal predittore stesso. In quanto supervised, le tecniche in questa famiglia possono essere applicate all’identificazione delle anomalie quando si rendono disponibili dati annotati sui quali addestrarle. In letteratura sono presenti molti risultati che usano machine learning alla rilevazione di anomalie nei settori applicativi più vari: le tecniche utilizzate variano dall’applicazione di *alberi di decisione* [Gaddam *et al.*, 2007], alle *support vector machines* fino all’uso delle reti neurali di diverse architetture: *feedforward neural network* (FNN), *convolutional neural network* (CNN) e *recurrent neural network* (RNN). Recentemente, le ultime due tipologie di rete sono state spesso utilizzate con efficacia per il riconoscimento di anomalie di diversa natura. Mentre le CNN sono state riconosciute come architettura di rete di riferimento per l’identificazione di anomalie su time series [Nanduri e Sherry, 2016], le seconde sono state efficacemente utilizzate in applicazione aeronautica per la predizione di anomalie su time series generate da sensori installati su turbine aeree [Malhotra *et al.*, 2015].

In questo articolo descriviamo i risultati di una collaborazione in atto tra: centro ricerca FCA (Orbassano, Torino), CNR di Pisa, Università di Pisa e Venezia, e INTECS (Pisa). La collaborazione ha come oggetto l’investigazione di metodi di apprendimento automatico per l’identificazione di anomalie su big data raccolti sul *CAN bus* di autovetture di test FCA.

## 2 Ricerca di anomalie: metodologia

I dati registrati sul *CAN bus*, una volta ripuliti, si possono assimilare ad un insieme di serie temporali di valori numerici o categorici dove ogni serie è associata ad un dispositivo distinto. A differenza dei problemi di classificazione e regressione “classici”, nella predizione di serie temporali si presentano delle difficoltà aggiuntive: le dipendenze temporali tra le osservazioni. Si tratta di una caratteristica tanto importante quanto difficile da sfruttare. Inizialmente, per la predizione di serie temporali si impiegavano modelli lineari come ARIMA, caratterizzati da una grande semplicità ed applicabili per diverse classi di problemi. Purtroppo questi metodi falliscono in presenza di: i) dati mancanti e/o corrotti, ii) dipendenze non lineari tra i dati, iii) dati multivariati, iv) correlazioni con finestre temporali ampie. Queste caratteristiche sono presenti tutte, in forme molteplici, nei dati di riferimento di questo lavoro. D’altro canto, l’utilizzo di reti neurali con architettura profonda permette di affrontare problemi quali: la robustezza al rumore, con la possibilità di addestrare modelli di predizione anche in presenza di porzioni di serie mancanti; l’apprendimento di dipendenze non lineari tra i dati, con la possibilità di imparare dai dati funzioni anche molto complesse. Inoltre, queste reti permettono di gestire un numero arbitrario di serie temporali in input in modo da costruire modelli di predizione per dati multivariati. Per tutti questi motivi le reti neurali sono particolarmente indicate per l’identificazione di anomalie in questo ambito. L’analisi della letteratura ha evidenziato una particolare architettura di rete ricorrente (RNN) candidata ad essere usata: *Long-Short Term Memory Network (LSTM)* [Hochreiter e Schmidhuber, 1997]. Un’ulteriore conferma arriva dai risultati pubblicati negli ultimi anni: LSTM è impiegata in molti problemi di identificazione anomalie in diversi domini. Tali reti hanno registrato negli ultimi anni un grandissimo successo, grazie soprattutto alla grandissima quantità di dati ora a disposizione per il loro addestramento.

## 3 Esperimenti

I dati messi a disposizione da FCA monitorano i sensori installati sull’automobile registrandone i valori a istanti temporali fissati. L’analisi che mostriamo in questo articolo sfrutta i dati raccolti su due autovetture di test in un intervallo temporale di tre mesi. Le due macchine sono equipaggiate con lo stesso insieme di sensori. Per ogni sensore, ogni valore riportato è associato al relativo timestamp e quindi si rende possibile ricostruire la serie temporale dell’acquisizione. Un sottoinsieme di acquisizioni è stato etichettato da esperti FCA con annotazioni relative ad un comportamento anomalo di uno specifico sensore. Tali serie annotate sono incluse nel test set usato per verificare l’accuratezza dei modelli addestrati. La rete LSTM che descrive il “normale” funzionamento dell’autovettura è invece addestrata su tutte le acquisizioni fornite ad esclusione delle osservazioni, positive e negative, incluse nel test set. Il modello ottenuto consente di predire i valori futuri di un insieme di serie temporali dati i valori delle serie nella finestra temporale precedente. Il comportamento anomalo è identificabile quando l’errore misurato tra il comportamento predetto dal modello e la serie temporale reale è ampio. Un semplice esempio illustrativo è riportato in Figura

1 dove, in blu, sono riportati i valori di un sensore che misura l’apertura della portiera del guidatore del veicolo e, in arancio, i valori predetti dal modello al variare degli istanti temporali di registrazione (asse X). Si può osservare che la portiera risulta aperta nell’intervallo evidenziato in rosso. Da un’analisi degli altri segnali si è osservato che il veicolo in quella finestra temporale era in movimento e che quindi la portiera aperta è da considerarsi un comportamento anomalo del sensore. La rete LSTM è qui in grado di evidenziare il problema con predizioni discordanti nell’intervallo evidenziando l’anomalia in questione.

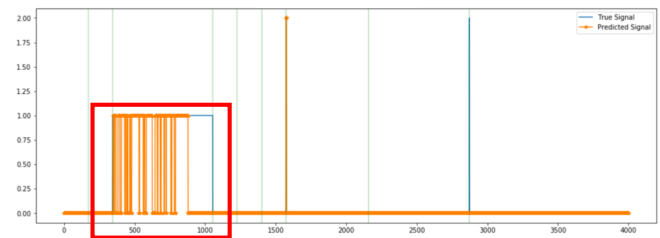


Figura 1: Esempio di comportamento anomalo (riquadro rosso) del sensore *portiera guidatore*. In questo esempio la rete LSTM (linea arancio) è in grado di evidenziare correttamente l’anomalia.

L’esempio in Figura 1 suggerisce che allo scopo di identificare le anomalie si possano definire strategie diverse. Tra quelle varie provate la strategia migliore è risultata essere quella che seleziona e aggrega i primi  $k$  segnali aventi il maggiore errore di predizione. Con questa strategia più segnali sono riportati ad un’unica anomalia quando essi fanno riferimento allo stesso sensore e sono registrate in istanti temporali vicini. Sono stati eseguiti diversi addestramenti finalizzati a ottimizzare tutti i parametri che governano l’efficacia finale della rete. Le reti addestrate con la strategia descritta sopra hanno accuratezza sul test set superiore al 75%. Il prototipo dell’ambiente di sviluppo e testing realizzato in ambito accademico è ora installato ed utilizzato presso il centro ricerche FCA di Orbassano. Il progetto è inoltre stato premiato con un NVIDIA Academic Grant che ha visto la fornitura gratuita di una scheda video Titan Xp al CNR di Pisa.

## Riferimenti bibliografici

- [Gaddam *et al.*, 2007] Shekhar R Gaddam, Vir V Phoha, e Kiran S Balagani. K-means+ id3: A novel method for supervised anomaly detection by cascading k-means clustering and id3 decision tree learning methods. *IEEE transactions on knowledge and data engineering*, 19(3):345–354, 2007.
- [Hochreiter e Schmidhuber, 1997] Sepp Hochreiter e Jürgen Schmidhuber. Long short-term memory. *Neural computation*, 9(8):1735–1780, 1997.
- [Malhotra *et al.*, 2015] Pankaj Malhotra, Lovekesh Vig, Gautam Shroff, e Puneet Agarwal. Long short term memory networks for anomaly detection in time series. In *Proceedings*, page 89. Presses universitaires de Louvain, 2015.
- [Nanduri e Sherry, 2016] Anvardh Nanduri e Lance Sherry. Anomaly detection in aircraft data using recurrent neural networks (rnn). In *2016 Integrated Communications Navigation and Surveillance (ICNS)*, pages 5C2–1. IEEE, 2016.