Noise Injection/ Machine Learning Fraud Detection Framework in Time Series Data

Article · January 2019

CITATIONS
0

READS
66

3 authors:

Aris Magklaras
University of Patras
6 PUBLICATIONS **35** CITATIONS
SEE PROFILE

Nikolaos Andriopoulos
University of Patras
10 PUBLICATIONS **51** CITATIONS
SEE PROFILE

Alexios N. Birbas
University of Patras
135 PUBLICATIONS **1,130** CITATIONS
SEE PROFILE

Noise Injection/ Machine Learning Fraud Detection Framework in Time Series Data

Aristeidis Magklaras, Nikolaos Andriopoulos, Alexios Birbas
Department of Electrical and Computer Engineering
University of Patras
Patras, Greece, 26500

***Abstract*—Internet connectivity (IoT) of ever increasing numbers of physical sensing devices, results in vast amounts of sensing (measurement) data which have to be transmitted and processed in order to extract information. Data exchange and manipulation raise several concerns regarding privacy, security and integrity of the measurement data (i.e electricity smart meters). Noise injection into the measurement time-series data is proposed in order to enhance data resilience. This noise injection in combination with statistical analysis tests while operating in a machine learning framework enables the detection of malicious data (fraud detection) in the receiver. Statistical analysis is essential in the case of time-series data collection, since the statistical properties of any time-series can give a strong indication of whether the data is being maliciously changed or not.**

***Index Terms*—noise injection, white noise, Poisson distribution, fraud detection, machine learning, time-series statistical analysis**

I. Introduction

The number of IoT devices has increased exponentially during the last few years. Nowadays, terabytes of data are exchanged on a daily basis between several smart devices [1] and according to [2] by the end of 2020 there will be between 20 and 50 billion devices connected. The high frequency of transactions and the huge amount of data transferred causes an increased vulnerability regarding private data sensitivity as well as transactions security and integrity. Between the applications that are benefited from the IoT development is remote smart metering; a possible loss of measured data integrity and privacy would result in costly defects. For example, in the case of electrical energy application at the Utility level, data integrity loss might imply energy theft and set the whole Utility system stability into danger. Rajagopalan et. al [3] describe the problem of IoT deployment as a trade-off between Utility and privacy. Nevertheless, IoT opens opportunities for new services provision, despite the raising of important data related concerns.

There have been several attempts and many different approaches to leverage the data integrity problem. In [4] an on demand security configuration of the IoT device is being proposed, while in [5] a similar, remote configuration of the aggregator internet server is introduced. In [6] the modification and extra hardware configuration of IoT devices is proposed, and despite the cost and complexity of this solution, there already exist several low-end IoT devices serving this purpose. Given that all of the aforementioned solutions require the usage of either complicated and more expensive devices or at least the modification off the software of the current devices (which is also inefficient on most scenarios). In this work, we consider a different approach, that of injecting noise in the measured time-series data without the need to modify the hardware or the software of the device.

Time-series of measurement data can be regarded as progression of various shapes in time. Noise, that is usually of certain type and color, is inherent in time-series or can be artificially introduced. Artificially injected noise is a viable solution not only for protecting the data from being hacked, but also for enhancing the integrity and security of transactions made between connected devices. Several interesting solutions have been introduced which manage to reverse the negative effects of noise into an adhesive data resilience tool. Noise injection in the measurement data (time-series) is a first order solution for fraud detection if the statistical characteristics are known at the signal receiving part [7]. In [8], a light privacy model with noise injection in the data is presented in order to limit the risk of hacking. Only the masked, noise injected data are transferred outside of the device. The investigation of non-stationarity and the classification of specific events in noisy time series data [9] are used for the analysis of the received signal. If the received data (time-series) are altered to some degree by noise, the investigation of noise characteristics are an effective method for fraud detection. Our method enhances the ability to estimate the degree of noise corruption, by examining specific statistical characteristics, such us non-stationarity.

The proposed methodology is most suitable for smart grid load measurement data, where noise injection in the data series at the smart meter side is combined with statistical analysis and machine learning algorithms at the receiving end of the energy aggregator. This analysis leads to conclusion about data validity. The proposed methodology enhances the secure transaction between IoT devices, while preserving data privacy.

II. Proposed Methodology

The usual approach for studying various structures in time-series analysis is to assume that a certain process with

known statistical/ physical characteristics results to a specific, recognizable, temporal trace. Detecting such a trace in the time-series one can conclude regarding the data integrity and recognition. In this work, white noise with known statistical properties and characteristics is the physical injection mechanism for detecting malicious data. The white noise process is one of the usually involved type of noise for direct detection of malicious data. When adding white noise to a signal, the frequency spectrum of the resulting signal remains the same with the original one. A white noise process is defined by the following equation:

$$S_w(\omega) = N_0/2 \tag{1}$$

where N_0 is a real constant and called the intensity of the white noise. This exact characteristic of white noise combined with the statistical analysis of the electric load signal enhances the ability to detect any potential fraud or malfunction of the system. The proposed methodology is shown in Fig.1. At first, the smart meter emits an encrypted signal which is a superposition of the measurement and white noise data (with specific characteristics, so that to achieve an SNR unique for each different smart meter). The encryption process deals only with white noise data injection, thus the fundamental frequency remains unchanged.

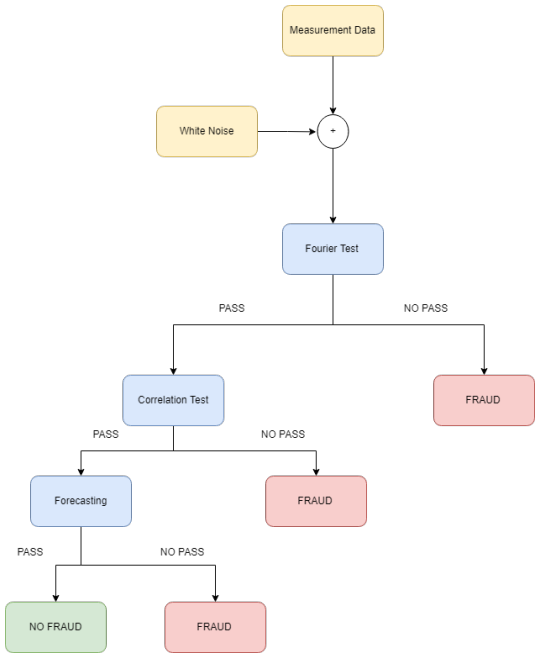

Fig. 1. The proposed methodology

The encrypted signal has the shape shown in Fig.2 (encrypted with the addition of white noise).

At the receiver side, a Fourier test over the time series is applied in order to detect any malfunction or intrusion over the received signal. Fourier test enables the detection of any change in the fundamental frequency and leads to a conclusion whether there has been a possible fraud over the signal or

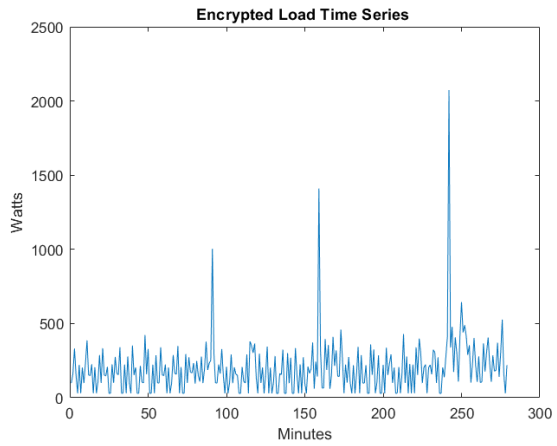

Fig. 2. White Noise Encrypted Load Time Series Data

not. Failing the Fourier test implies that the measurement data were mixed with false data and for this reason the algorithm classifies this transaction as a fraud. Fig.2 and Fig.3 portray two different noise injections in originally measured time-series data. In Fig.3 the injected noise data follow a Poisson distribution and in Fig.2 the injected data follow a normal distribution resembling white noise.

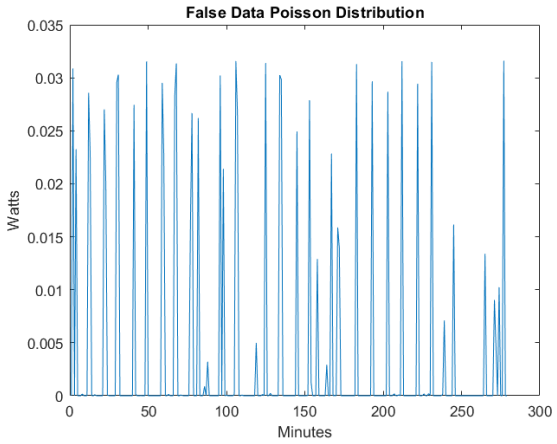

Fig. 3. Poison Noise Encrypted Load Time Series Data

Fig.4 presents the power spectral density of the initial, measured time-series data, which is unaltered in the case of white noise injection (as shown in Fig.5). Since the fundamental frequency remains unchanged under white noise injection, we have experimented with non white noise injection (Poissonian noise). In this case the frequency spectrum is different than expected as shown in Fig.6 and we drive the conclusion that the transaction can be classified as a fraud.

The second step of the framework addresses the possibility of having fraud data injection that follows a normal distribution (white noise), thus making harder and more difficult to detect any malfunctions. In this case the statistical property of auto-correlation is employed as the indicative feature en-

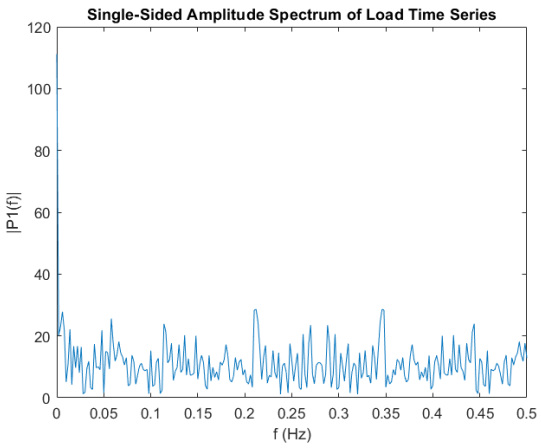

Fig. 4. Frequency Analysis Load Time Series Data

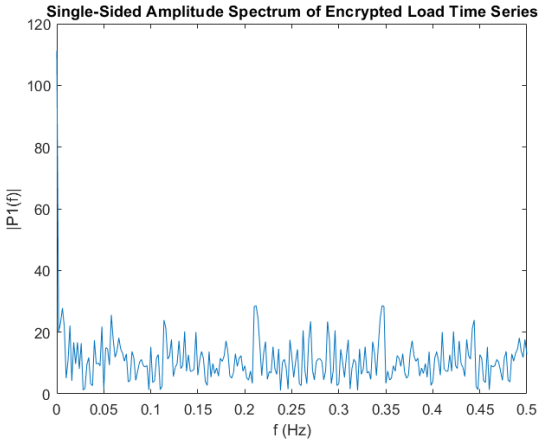

Fig. 5. Frequency Analysis of White Noise Encrypted Load Time Series Data

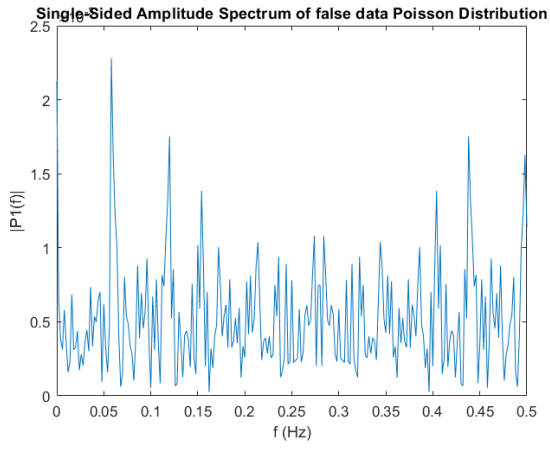

Fig. 6. Frequency Analysis of Poison Noise Encrypted Load Time Series Data

abling the detection of a potential fraud. In case of malicious injection the correlation factors of the received time-series is altered. The correlation characteristics of the received time series is compared with archival time series available at the receiver/aggregator side. In Fig.7 the auto-correlation plot of an example electric load time-series data is shown.

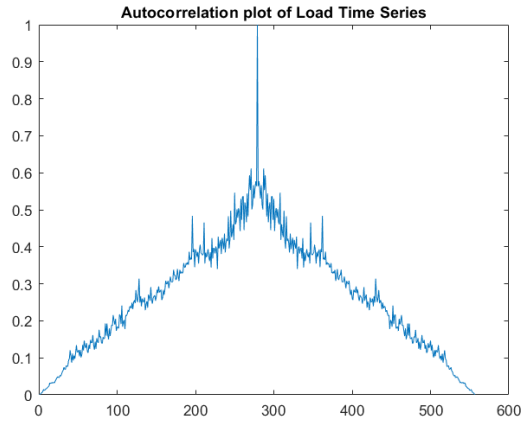

Fig. 7. Auto-correlation Plot of Load Data

Apart from the auto-correlation of the time-series itself, the correlation between different time-series could provide metrics for comparison. If we continue with examining the electric load data we can observe in Fig.8 and Fig.9 that the correlation between electric load and A1 RMS (electric current measurement) or Vthd (Voltage total harmonic distortion) also follows a specific pattern. For this reason, it is almost impossible for someone to inject data by correctly imitating the correlation patterns for all those different measurements.

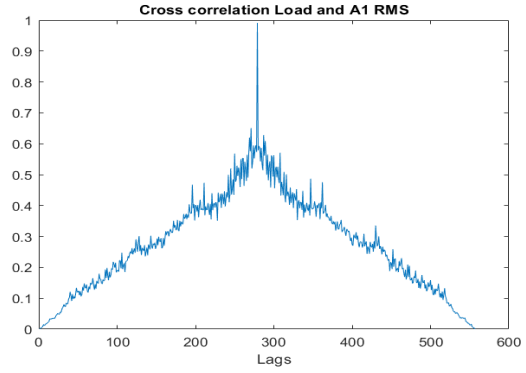

Fig. 8. Cross Correlation Electric Load and A1 RMS

At this point our decision tree methodology already has strong indications of fraud or not but we still need to confirm the result with a final step which is a machine learning based forecasting tool. If the Mean Absolute Percentage Error (MAPE) between the new time series and our forecasted values is higher than of our model, and at the same time the correlation tests fails, then the data is classified as a fraud. In case of only failing either the forecasting or the correlation test, then the new signal is classified as a possible fraud.

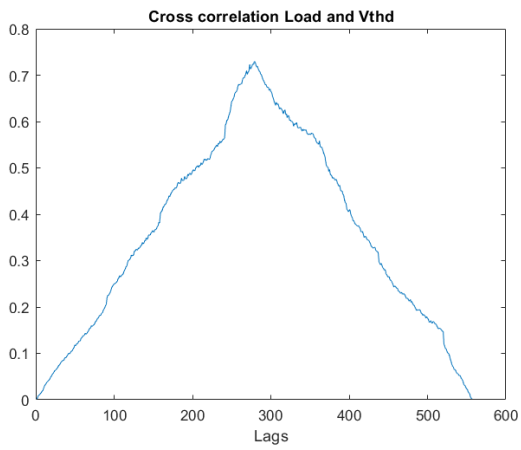

Fig. 9. Cross Correlation Electric Load and Vthd

III. Conclusions

The huge amount of data transferred and the expansion of IoT devices in almost every aspect of our life raises extremely important concerns regarding the security and privacy of several sensitive information (data). Since hacking into the hardware requires specific knowledge, false data intrusion can be seen as a more realistic threat regarding for example the energy data acquired from smart meters. By employing data analysis and novel machine learning techniques, those potential malfunctions can be addressed more efficiently in terms of cost and time. The fact that changing the hardware of IoT devices is not a realistic scenario, the exploitation of data analysis and novel machine learning techniques is the most efficient method to tackle these issues. As examined in this work this is a solution that can provide as with robust results, especially for time-series data which have a physical meaning (the electric load measurements). In this case the statistical analysis and the expected results can be used in order to precisely detect a fraud or not.

References

[1] D. Evans, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything", Cisco Internet Business Solutions Group (IBSG), pp. 1-11.

[2] Gartner, "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015.", November 10, 2015, http://www.gartner.com/newsroom/id/3165317 (accessed June 24, 2016).

[3] Rajagopalan, S. R., Sankar, L., Mohr, S., and H.V Poor, " Smart meter privacy: a utility-privacy trade-off framework", IEEE 2nd Intl. Conf. Smart Grid Commun., Brussels, (Oct. 17-27, 2011), pp.150-155.

[4] Chung, B., Kim, J., and Jeon, Y. (2016)," On-demand security configuration for IoT devices", 2016 International Conference on Information and Communication

[5] Yoon S., and Kim J., "Remote security management server for IoT devices", 2017 International Conference on Information and Communication Technology Convergence

[6] Steven J. Johnston, Mark Scott, Simon J. Cox, "Recommendations for securing Internet of Things devices using commodity hardware",2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)

[7] Nyemkova E., "Invariants of noise in cyber-physical systems components",ACPS. 2017, Volume 2, Number 2, pp. 63-70

[8] P.Barbosa, A. Brito, H. Almeida, S. Clauss, "Lightweight privacy for smart metering data by adding noise", 29th Annual Symposium in Applied Computing, pp. 531-538 .

[9] T. Borgohain, U. Kumar,S. Sanyal, "Survey of Operating Systems for the IoT Environment", arXiv preprint arXiv:1504.02517, 2015