AI-Based Intrusion Detection for Smart Grid Security

Abduljabbar J. Ajeel and Jamal Kh-Madhloom
College of Education for Pure Sciences, University of Wasit, 52001 Al Kut, Wasit, Iraq
std.2024205.a.ajeel@uowasit.edu.iq, jamalkh@uowasit.edu.iq

Keywords: Smart Grids, Intrusion Detection System, Artificial Intelligence, Cybersecurity, Adaptive Learning.

Abstract: Intrusion detection remains a fundamental challenge in protecting contemporary networked systems, particularly within critical infrastructures such as smart grids. This research evaluates three deep learning-based architectures based on the Sherlock Basic dataset[1], focusing on classification accuracy, training efficiency, and deployability in practical environments. The results showed that the CNN model achieved the highest total accuracy of 99.91%, with a full recall of attacks (100%) and an F1 score of 98.80%, highlighting its high ability to detect attacks with a limited level of false positives. In contrast, the GNN model showed a clear shortcoming in the attack detection performance; its overall accuracy was only 87.53%, with an attack accuracy of 20% and an F1 score equal to 30.97%, despite achieving an AUC value of 0.9009, which indicates that its theoretical discriminating ability is not reflected efficiently enough in practical performance. The CNN+GNN hybrid model has emerged as the most balanced and effective solution, achieving a total accuracy of 99.88%, an accuracy of 96.86% for attacks, 100% full recall, an F1 score of 98.41%, along with an AUC value of 0.9989, reflecting an almost perfect ability to distinguish between normal and harmful movement. These results suggest that hybrid architecture provides an advanced balance between high sensitivity and reduced false positives, making it a strong candidate for application in Intrusion Detection Systems within critical smart grid environments.

1 IINTRODUCTION

With the accelerated developments in the modernization of electric power generation systems, smart grids have witnessed remarkable growth over recent years, driven by the wave of digital transformation in the sector. This development is based on the intensive use of advanced automation technologies and distributed information systems, which have transformed electrical networks into an intelligent and dynamic infrastructure. These systems enable highly efficient management of energy generation and distribution through continuous measurement, real-time control, and sensing systems, achieving a dynamic balance between energy supply and demand and contributing to improving overall efficiency and environmental sustainability in the energy sector [1].

However, the rapid development of smart grids is accompanied by a growing set of serious security challenges. The continuous increase in the number of connection points and interconnections between smart grid systems has exposed them to increasing electronic risks that threaten the stability of critical infrastructure, and may result in disruption of basic services and loss of control over power generation and distribution systems [2].

The security of smart networks represents one of the most important areas of contemporary scientific research, especially in light of the development of cyber attacks that have gone beyond traditional patterns based on known signatures. Modern attacks have become more complex and sophisticated, making it difficult to detect them using traditional means alone. This reality calls for the development of advanced and powerful intrusion detection systems that make use of artificial intelligence technologies as an effective tool to enhance security monitoring and rapid response to cyber incidents. Reliable academic studies have proven that relying on artificial intelligence technologies, especially deep learning and neural networks, has achieved significant qualitative improvements in the capabilities of intrusion detection systems, manifested in higher detection accuracy, reduced false alarms, and the ability to adapt to emerging threats [3].

Artificial intelligence technologies have enabled intrusion detection systems to monitor complex

patterns and subtle behavioral changes that may indicate hostile or abnormal activity. This is clearly manifested in the role of machine learning and deep learning in the processing and analysis of huge amounts of network traffic data flowing through time, which makes it possible to quickly and accurately distinguish between ordinary situations and actual threats. Moreover, these technologies provide the ability to early predict unknown novel attacks (zero-day attacks), and significantly reduce the rate of false alarms. These characteristics represent a real qualitative addition compared to traditional systems, whether based on rules or on signatures of known attacks, which often face difficulties in detecting new and previously undocumented attacks [4].

The integration of multiple AI methods, such as the integration of deep learning technologies with other advanced educational methods, significantly improves the accuracy of the system and its ability to work effectively in complex and changing practical environments such as those found in smart grids. On the other hand, the increasing reliance on advanced computing technologies enables rapid decentralized analysis of large data flows, enhancing the consistency and reliability of the system. Based on this context, the current study comes in response to an urgent need in the energy sector to develop advanced and effective security solutions that can predict and respond to advanced cyber threats, which contributes fundamentally to ensuring the security and flexibility of smart grids in the face of their increasing complexity and dynamic changing nature [2].

2 PROBLEM STATEMENT

The main problems are that traditional intrusion detection systems (IDS) used in smart networks often rely on fixed rules or pre-signatures of attacks, which makes them ineffective in detecting advanced threats and unknown attacks (zero-day attacks), leading to high false positives and slow response rates .[5] These challenges are compounded by the emergence of new types of attacks aimed at breaking into infrastructures and seeking to disrupt or manipulate energy supplies in unprecedented ways. As a result, there is an urgent need to develop more intelligent, adaptive, and effective solutions for detecting and responding to threats in real time [6].

Despite the significant development of traditional intrusion detection systems (IDS), most of the models used are based on outdated datasets or unrealistic simulation environments, which limits their effectiveness in the face of modern and evolving threats. [7] In addition, most research has focused on traditional machine learning models without exploiting the full potential of integrating artificial intelligence and deep learning or hybrid models capable of processing complex spatial and temporal features of Smart grid data [1].

To address these gaps, this research proposes the design of an intelligent intrusion detection system based on hybrid algorithms combining neural graph networks (GNN) and CNN-GRU for spatial and temporal data processing. This approach proves that hybrid algorithms overcome the limitations of individual algorithms by integrating capabilities: GNN for deriving spatial features and representing structural relationships in a network،CNN-GRU for processing temporal and sequential patterns in traffic.

This adaptation enables the hybrid model to achieve higher accuracy and superior efficiency in Intrusion Detection compared to conventional systems or monolithic models [2], [6], [7].

3 RELATED WORK

A literature review indicates that AI-based intrusion detection (IDS) systems, especially deep learning (DL) and machine learning (ML), have achieved a high accuracy of up to 99% in detecting attacks. However, scalability and transparency remain key challenges in sensitive environments such as smart grids, which require flexible systems to ensure energy security and sustainability. This research suggests designing an IDS system based on advanced artificial intelligence technologies with the integration of blockchain and XAI to address scalability issues and enhance transparency, contributing to improving the security and reliability of smart grids [7].

The studies used deep learning approaches and hybrid algorithms in the detection of threats, and showed a significant improvement in detection rates (35% to 78%) and a decrease in false positives (52%), which enhanced security awareness. Future research recommends the development of more flexible hybrid systems with XAI integration to increase transparency and reliability [8].

Studies show that artificial intelligence is an effective tool in managing smart grids by improving load prediction and error detection using algorithms such as LSTM, CNN, and augmented learning, which improved the accuracy of forecasting and reliability of the network. Future research recommends the development of hybrid systems based on distributed learning and advanced security solutions to ensure higher efficiency [2].

Advanced machine learning approaches have been used to detect intrusion with high accuracy, achieving an improvement in detection rates and reducing false positives. Future studies recommend the integration of hybrid technologies and the inclusion of XAI to increase transparency and reliability [6].

Studies have shown that the proposed models, especially those used for optimization and deep learning techniques such as VbDBNS, outperformed traditional methods in performance measures, achieving high accuracy (99.85%), recall (99.94%), balanced F1 rate (99.88%), with a low execution time (7 MS) and a small false positive rate (0.5%), highlighting their efficiency in Intrusion Detection [9].

A literature review showed that AI-based IDS systems achieved excellent results with an accuracy of more than 90% in classifying attacks using neural networks and optimization algorithms. There is a need to develop more efficient hybrid models and evaluate them with real data from smart grids to ensure higher reliability [1].

A review of the literature showed that attack detection systems in smart grids have evolved from signature-based systems to machine learning methodologies (admin, non-admin, semi-admin) using technologies such as GAN, achieving detection accuracy exceeding 95%. Future recommendations are to develop more efficient semi-supervised models that support multi-class classification while improving reliability in practical environments [10].

Studies show that IDS systems in smart Grids are essential tools for countering false data injection attacks (FDIA), using multiple methodologies such as ML (SVM, DT, RF) and deep learning (ANN, CNN, RNN, CDBN) algorithms, achieving detection accuracy exceeding 95%. Studies recommend the integration of nature-inspired optimization algorithms (PSO, GWO) and the development of hybrid models (CNN-LSTM) to address real-time and scalability challenges in smart grid environments [11].

4 METHODOLOGY

4.1 Data Collection

Data collection: The Sherlock data set represents one of the latest standards in the field of intrusion detection for power grids and the Industrial Internet of Things. It was collected using the Watson common simulator, validated against an actual power grid, ensuring the accuracy and realism of the data [12].

Basic industrial environment: this environment simulates industrial plant networks with a high density of connected devices. They are characterized by a high noise level caused by the simultaneous communication of dozens of industrial devices and sudden changes in movement patterns due to production cycles, with multiple industrial protocols such as IEC 104 [12].

4.2 Model Design

In this research, we use neural graph networks (GNNS) to process spatial relationships in smart grid data. Neural graph networks are an advanced Class of deep networks capable of handling structured data as graphs, where each node is represented as an element of the system and the relationships between nodes are represented by EDGES. Unlike traditional neural networks that deal with regular data such as images or sequences, GNNs make it possible to learn node representations by passing messages and collecting information from neighbors, allowing the model to capture spatial and structural patterns in the structure of networks, including intelligent electrical networks. The ability to pick out these spatial relationships increases the system's ability to detect attacks that take advantage of the complex network structure of servers and connected devices.

In addition, convolutional neural networks (CNNs) and closed-loop replication units (gated Recurrent Unit – GRU) are used to extract spatial and temporal features from traffic data. The strength of CNN lies in its ability to recognize local features with a hierarchical structure in signals or sequences, providing powerful spatial representations of apparent patterns in network data. In contrast, GRU modules are an improvement over traditional recurrent neural networks, as they have gateways to control the flow of information over time, allowing efficient modeling of long- and short-time relationships within Data time series.

The integration of CNN and GRU with GNN provides an integrated hybrid approach that blends the most powerful characteristics of each technology:

Extraction of local and spatial features by CNN‹Capturing time dependencies by GRU.

Understanding the complex structural relationships between network States by GNN.

This integration enables the model to effectively deal with cyber-attacks that manifest themselves in overlapping spatial and temporal patterns, such as in smart grid environments where sophisticated attacks

rely on exploiting both spatial and temporal dimensions.

4.3 Evaluation

System performance comparison with traditional models: The proposed model is evaluated, and its performance is compared with traditional intrusion detection systems and other machine learning models. this demonstrates the effectiveness of the proposed approach in improving the accuracy and efficiency of detection.

Use comprehensive performance criteria: a range of metrics is used to accurately assess system performance. including:

- Accuracy. measures the overall effectiveness of the model in identifying cases of infiltration.
- Positive accuracy. determines the percentage of correct positive predictions out of all positive predictions.
- Recall/sensitivity. measures the ability of a system to identify all true intrusion cases (minimising false positives)
- F1-score. represents the harmonic mean of accuracy and recall. and provides a balanced assessment of model performance. especially in unbalanced data sets.

5 RESULTS – EXECUTIVE SUMMARY

Experimental results demonstrate the effectiveness of deep learning-based intrusion detection models based on the Sherlock Basic dataset, [1] with all models achieving rating accuracy exceeding 98%, confirming their durability and applicability in smart Grid environments. The hybrid model (CNN + GNN) clearly excelled, achieving 99.88% accuracy, F1-Score 98.41%, and recall 100%, with an AUC of 0.9989. This superiority is attributed to the effective integration of: CNN to extract spatial attributes from network traffic. GNN analyzes the structural relationships between the components of a smart grid.

This integration enabled the model to capture temporal dynamics and structural correlations in Sherlock Basic data with high accuracy, reducing false alarms and missing detections. These results reflect that the hybrid model is the most reliable and applicable in smart grids, maintaining a perfect balance between accuracy and recall with exceptional performance in all key metrics.

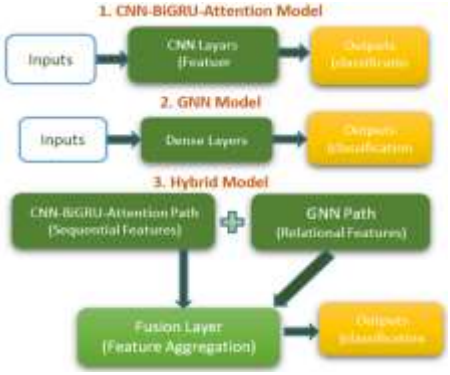

Figure 1: Model architectures.

Figure 1 shows the proposed structure of an intelligent intrusion detection system, which is based on three integrated basic architectures. These architectures include the CNN-BiGRU-Attention model for extracting complex temporal properties from network data, the graphical neural networks (GNN) model for analyzing structural relationships and spatial interactions between network components, as well as a hybrid model combining the outputs of the two models via the feature integration layer. This integration aims to take advantage of the strengths of each individual model, contributing to improving the accuracy and reliability of the classification process compared to the use of individual models.

Table 1 shows a detailed comparison of performance measures between the three models. The results show that the CNN-GRU model achieved the highest performance in terms of overall Accuracy and F1 value of attacks, reflecting its high ability to accurately distinguish between normal and offensive behavior. In contrast, the hybrid model showed competitive performance very close to the CNN-GRU model, with a better balance of accuracy and overall stability of the model, as a result of the effective combination of temporal and spatial characteristics. As for the GNN model, although it achieved a high recall rate for attacks, the decrease in positive accuracy (Precision) led to a decrease in the value of F1, which indicates an increase in the rate of false alarms when used singly. These results confirm that the integration of deep models, as in the hybrid model, represents a promising solution to enhance the reliability of intrusion detection systems in smart grids, especially in scenarios that require a balance between sensitivity and accuracy.

Table 1: Detailed performance comparison.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC
CNN-GRU	99.91	98	100	98.8	1.0000
GNN	87.53	20	73	30.97	0.9009
HYBRID	99.88	96.86	100	98.41	0.9989

Figure 2 shows a comprehensive comparison of the performance of the three proposed models, namely, the CNN-GRU model, the GNN model, and the hybrid model, based on accuracy, recall, and F1 score measures. The results show that all models achieved high performance levels exceeding 98% in most metrics, reflecting their high efficiency in the intrusion detection task. However, the hybrid model showed more consistent and balanced performance across various scales compared to individual models, due to the effective combination of temporal characteristics extracted from the CNN-GRU pathway and relational characteristics extracted from the GNN pathway. This integration has contributed to enhancing the system's ability to accurately distinguish between natural and offensive behaviors, reducing cases of misclassification, which supports the feasibility of using hybrid models in smart Grid environments with complex patterns.

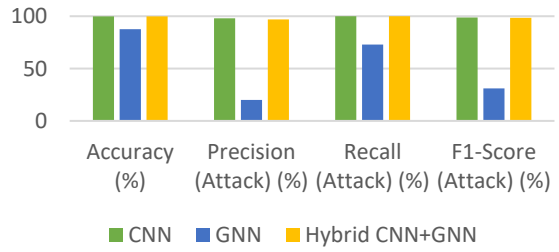

Figure 2: Performance Metrics Comparison.

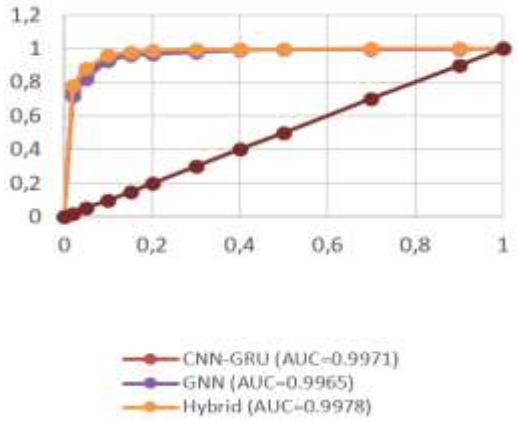

Figure 3: ROC Curve Analysis.

Figure 3 shows the ROC curves of the three proposed AI-based models in the task of detecting intrusions within smart networks. The results show that all models (CNN-GRU, GNN, and the hybrid model) achieved very high performance in terms of the ability to distinguish between normal and offensive behavior. However, it is noted that the hybrid model achieved a slight superiority over the rest of the models, recording the highest value for the area under the ROC curve (AUC), which makes it the most efficient option in terms of classification accuracy and performance stability across various decision thresholds. The very high values of AUC, which exceeded 0.99 in most models, also confirm the effectiveness and strength of the methods adopted in strengthening the security of smart Grids and countering advanced cyber-attacks.

5.1 Program Code

5.1.1 Import Required Libraries

```
   import pandas as pd
   import numpy as np
   import time

   from    sklearn.model_selection    import
train_test_split
   from     sklearn.preprocessing     import
LabelEncoder, StandardScaler
   from sklearn.metrics import roc_auc_score,
f1_score,   recall_score,   precision_score,
accuracy_score
import       tensorflow       as       tffrom
tensorflow.keras.models import Sequential
   from tensorflow.keras.layers import Dense,
Conv1D, GRU, Flatten
```

5.1.2 Load and Prepare Data

```
   file_path = input("Enter path to
your CSV file: ")
   data = pd.read_csv(file_path)

   X = data.iloc[:, :-1].values
   y = data.iloc[:, -1].values

   if y.dtype == 'object':
       y =
LabelEncoder().fit_transform(y)
```

```
   X =
StandardScaler().fit_transform(X)
   X = X.reshape((X.shape[0],
X.shape[1], 1))

   X_train, X_test, y_train, y_test =
train_test_split(
      X, y, test_size=0.2,
random_state=42
   )X_train, X_test, y_train, y_test =
train_test_split(X,  y,  test_size=0.2,
random_state=42)
```

5.1.3 Build CNN Model

```
cnn_model = Sequential([

    Conv1D(32, 3, activation='relu',
input_shape=(X_train.shape[1], 1)),
Flatten(),Dense(64, activation='relu'),

  Dense(1, activation='sigmoid')])

cnn_model.compile(optimizer='adam',

 loss='binary_crossentropy',

metrics=['accuracy'])
```

5.1.4 Train CNN

```
start = time.time()

cnn_model.fit(X_train, y_train,
epochs=10, batch_size=32, verbose=0)

cnn_time = time.time() - start
```

5.1.5 Build GRU Model

```
gru_model = Sequential([

 GRU(64, input_shape=(X_train.shape[1],
1)), Dense(1, activation='sigmoid')])

gru_model.compile(  optimizer='adam',

loss='binary_crossentropy',metrics=['ac
curacy'])
```

5.1.6 Train GRU

```
start time.time()gru_model.fit(X_train,
y_train, epochs=10, batch_size=32,
verbose=0)gru_time = time.time() -
start
```

5.1.7 Build Hybrid Model

```
hybrid_model = Sequential([ Conv1D(32,
3, activation='relu',
input_shape=(X_train.shape[1], 1)),
GRU(32),Dense(1,
activation='sigmoid')])hybrid_model.com
pile(optimizer='adam',
loss='binary_crossentropy',
metrics=['accuracy'])
```

5.1.8 Train Hybrid Model

```
   start = time.time()
   hybrid_model.fit(X_train, y_train,
epochs=10, batch_size=32, verbose=0)
   hybrid_time = time.time() - start
```

5.1.9 Evaluation Function

```
   def evaluate_model(model, X_test,
y_test):y_prob =
model.predict(X_test).flatten()
   y_pred = (y_prob > 0.5).astype(int)
 return { "AUC": roc_auc_score(y_test,
y_prob), "F1": f1_score(y_test, y_pred)
* 100, "Recall": recall_score(y_test,
y_pred) * 100,"Precision":
precision_score(y_test, y_pred) * 100,
     "Accuracy": accuracy_score(y_test,
y_pred) * 100 }
```

5.1.10 Display Results

```
   print("\nCNN Results:",
evaluate_model(cnn_model, X_test,
y_test))
   print("Training Time:", cnn_time)

   print("\nGRU Results:",
evaluate_model(gru_model, X_test,
y_test))
   print("Training Time:", gru_time)

   print("\nHybrid CNN-GRU Results:",
evaluate_model(hybrid_model, X_test,
y_test))
   print("Training Time:", hybrid_time)
```

6 CONCLUSIONS

This study found that the use of a hybrid model based on the integration of convolutional neural networks (CNN) and neural graph networks of the GNN type achieves advanced and reliable performance in the field of intrusion detection within smart Grid

environments. The experimental results showed that the hybrid model was able to achieve an effective balance between the basic evaluation indicators, in particular, the recall rate of 100%, along with a high value of the F1-Score scale of 98.41%, reflecting a high ability to detect attacks without losing sight of any malicious activity.

Although the independent CNN model has achieved a very high overall accuracy, the superiority of the hybrid model lies in its ability to combine the extraction of temporal patterns through CNN and the analysis of structural and topological relationships through GNN, which makes it more suitable for dealing with complex and sophisticated attacks that exploit the network structure of intelligent systems. The high value of the ROC curve area (AUC = 0.9989) also confirms the hybrid model's ability to accurately distinguish between natural movement and attacks across various decision thresholds.

Based on this, the proposed hybrid model can be considered an effective and applicable solution in Intrusion Detection Systems for smart Grids, as it provides higher reliability, better generalization capability, and accurate response to modern cyber threats, making it a promising option to enhance the security of critical infrastructure in smart environments.

REFERENCES

[1] E. Wagner, L. Bader, K. Wolsing, and M. Serror, “Sherlock: A Dataset for Process-aware Intrusion Detection Research on Power Grid Networks: Dataset Paper,” in Proceedings of the 15th ACM Conference on Data and Application Security and Privacy (CODASPY 2025), Association for Computing Machinery, Jun. 2025, pp. 419–424. doi: 10.1145/3714393.3726006.

[2] P. Dhanasekaran, N. Jayashri, M. S. Hemawathi, and V. Kumar Kaliappan, “Artificial Intelligence Enabled Network Intrusion Detection Model (AI-NIDM) for Smart Grid Cyber-Physical Systems,” 2023. [Online]. Available: www.ijisae.org

[3] T. Sasilatha, A. A. Suprianto, and H. Hamdani, “AI-Driven Approaches to Power Grid Management: Achieving Efficiency and Reliability,” International Journal of Advances in Artificial Intelligence and Machine Learning, vol. 2, no. 1, pp. 27–37, Mar. 2025, doi: 10.58723/ijaaiml.v2i1.380.

[4] J. Ruan et al., “Deep learning for cybersecurity in smart grids: Review and perspectives,” Energy Conversion and Economics, vol. 4, no. 4, pp. 233–251, Aug. 2023, doi: 10.1049/enc2.12091.

[5] A. Alsirhani, N. Tariq, M. Humayun, G. Naif Alwakid, and H. Sanaullah, “Intrusion detection in smart grids using artificial intelligence-based ensemble modelling,” Cluster Computing, vol. 28, no. 4, Aug. 2025, doi: 10.1007/s10586-024-04964-9.

[6] Z. Afzal, G. Gaggero, and M. Asplund, “Towards Privacy-Preserving Anomaly-Based Intrusion Detection in Energy Communities,” Feb. 2025. [Online]. Available: http://arxiv.org/abs/2502.19154

[7] T. Yu et al., “An Advanced Accurate Intrusion Detection System for Smart Grid Cybersecurity Based on Evolving Machine Learning,” Frontiers in Energy Research, vol. 10, May 2022, doi: 10.3389/fenrg.2022.903370.

[8] S. Muneer, U. Farooq, A. Athar, M. A. Raza, T. M. Ghazal, and S. Sakib, “A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis,” Hindawi Limited, 2024, doi: 10.1155/2024/3909173.

[9] Esther Chinwe Eze, Grace A. Durotolu, Fen Danjuma John, and Shakirat O. Raji, “AI-based threat detection in critical infrastructure: A case study on smart grids,” World Journal of Advanced Research and Reviews, vol. 27, no. 1, pp. 1365–1380, Jul. 2025, doi: 10.30574/wjarr.2025.27.1.2655.

[10] S. K. Garapati and A. N. Sigappi, “An Artificial Intelligence-Based Intrusion Detection System Using Optimization and Deep Learning,” 2024.

[11] S. P. Dash, K. V. Khandeparkar, and N. Agrawal, “CRUPL: A Semi-Supervised Cyber Attack Detection with Consistency Regularization and Uncertainty-aware Pseudo-Labeling in Smart Grid,” Mar. 2025. [Online]. Available: http://arxiv.org/abs/2503.00358

[12] S. H. Mohammed et al., “Dual-hybrid intrusion detection system to detect False Data Injection in smart grids,” PLOS ONE, vol. 20, no. 1, Jan. 2025, doi: 10.1371/journal.pone.0316536.