International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Hybrid Deep Learning and Distrust Model for Fault Detection in IoT Networks

Manh Hung Nguyen

Intelligent Computing for Sustainable Development Laboratory (IC4SD)
Posts and Telecommunications Institute of Technology (PTIT), Hanoi, Vietnam
mhnguyen[at]ptit.edu.vn,
nmh.nguyenmanhhung[at]gmail.com

Abstract: ***The proliferation of the Internet of Things (IoT) has led to an unprecedented integration of diverse sensors, driving innovation across numerous domains. However, the reliability and security of IoT networks are significantly challenged by the presence of faulty sensors. Traditional fault detection methods are inadequate to manage the scale and complexity of modern IoT environments. This paper addresses the challenge of identifying faulty sensors in large-scale IoT networks by proposing a hybrid fault detection model that integrates deep learning and distrust mechanisms. Tested on simulated Hanoi air pollution data, the model demonstrates high accuracy and effectiveness, surpassing traditional fault detection methods. This approach provides a scalable, efficient solution to enhance the reliability of IoT networks.***

Keywords: IoT network, faulty sensor detection, deep learning, distrust model, anomaly detection

1. Introduction

In the rapidly expanding realm of the Internet of Things (IoT), where a multitude of sensors communicate and interact seamlessly to enhance various aspects of daily life, the reliability and efficiency of these interconnected systems are paramount. IoT networks are integral to numerous critical applications, ranging from smart homes and healthcare to industrial automation and smart cities. However, the sheer scale and complexity of these networks introduce significant challenges, one of the most pressing being the automatic detection of faulty sensors.

Faulty sensors within an IoT network can disrupt operations, degrade performance, and compromise security, leading to severe consequences, especially in mission-critical applications. Traditional manual methods of fault detection are not only time-consuming and labor-intensive but also impractical given the vast number of sensors and the dynamic nature of IoT environments. Therefore, there is an urgent need for robust, automated solutions capable of identifying and addressing faults promptly and efficiently. The challenge of automatically identifying faulty sensors in IoT systems has garnered significant research attention. Existing studies can be broadly classified into two main approaches: machine learning-based methods and trust/distrust/reputation models. The first approach is Machine Learning-Based Methods. One prominent approach to detecting faulty sensors in an IoT network is to treat the problem as a type of anomaly detection on the data captured by the sensors. Various deep learning methods have been employed in anomaly detection, as surveyed of Landauer et al. [8], Pang et al. [18], Diro et al. [6], Chatterjee and Ahmed [5], Han et al. [7], a widely deep learning methods are used in anomaly detection problem, from Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Autoencoder (AE), Generative Adversarial Network (GAN), to Transformer (TF), Attention mechanism (AT), Graph Neural Network (GNN), Evolving Granular Neural Network (EGNN), etc... For instances, Zakariah and Almazyad [24] combined feature engineering methods, active learning approaches, and a random forest classifier to construct a resilient anomaly detection model for IoT sensors. Liu et al. [10] applied different machine learning algorithms to efficiently detect anomalies on the IoT Network Intrusion Dataset. Abusitta et al. [1] proposed deep learning model which is designed based on a denoising autoencoder, which is adopted to obtain features that are robust against the heterogeneous environment of IoT. In the work of Sahu and Mukherjee [20] different anomalies are predicted based on a different feature in the data set. Two machine learning classification models are used and comparisons between the performance of these used models are shown. Logistic regression and artificial neural network classification algorithms are applied. Alghofaili and Rassam [2] proposes a model for trust management in IoT sensors and services based on the simple multi-attribute rating technique (SMART) and long short-term memory (LSTM) algorithm. Ma et al. [11] proposed a machine learning empowered trust evaluation method: the trust properties of network QoS (Quality of Service) are aggregated with a deep learning algorithm to build a behavioral model for a given IoT sensor, and the time-dependent features of network behaviors are fully considered. Ali-Eldin [3] computed trust in social IoT scenarios using a hybrid approach that combines a distributed computation technique and a global machine learning approach.

The second main approach involves trust/distrust/reputation mechanisms, which have been applied across various fields, including e-commerce, social networks, and intelligent systems ([15], [16], [17], [23]). In which, trust can be estimated from the history of interactions (experience trust), from the evaluation of partners who have interacted in the past (reputation), or it can be a combination of both types of trust above. Therefore, trust is naturally applied to IoT systems by estimating the reliability of each sensor based on the captured historical data that the sensor sends back (a kind of experience trust), or may be based on interaction history/information sharing between sensors, if any (a kind of reputation). For instances, in the work of Nguyen [14],

the distrust level of a sensor is estimated based on the variance in its captured values. Prathapchandran and Janani [19] uses the logistic regression model to predict the node's behavior based on the integrated trust value which is computed from the direct trust, reputation score, and experience trust. Alsheakh and Bhattacharjee [4] present a roadmap towards building a unified approach towards establishing trust scores as an indicator of the security status of an IoT sensor in a smart home that works across multiple attacks and sensor types/protocols. Magdich et al. [13] propose a Trust Management model dedicated not only to identify trustworthy nodes, but also to detect and prevent malicious attacks. Macedo et al. [12] present a two-level approach to simultaneously consider application and network characteristics, in which trust is modeled by combining a relative entropy measure of sensor's data rate (at the low level), and a reputation of a sensor provided by distributed ledger (at the high level). Shakya [22] proposed a prototype that is used to determine the performance of the system by means of real-time input from the industries by extensive experimentation. Yao et al. [9] proposed an integrated fault diagnosis and fault tolerant control algorithm of nonlinear networked control systems.

The purpose of this study is to develop and evaluate a hybrid model combining deep learning and distrust mechanisms to improve faulty sensor detection in IoT networks. This model is a combination of a deep learning method to detect the anomaly data obtained from sensors, and a distrust model to estimate the distrust level of a sensor regarding its obtained data among other neighbor sensors.

The paper is organized as follow: Section 2 presents the proposed model which is combination of a deep learning technique and a distrust model to automatically detect the error sensors in an IOT network; Section 3 presents the experiments and evaluation of the proposed model on a simulated system; Section 4 is the conclusion.

2. Proposed method

The general architecture of the proposed model is depicted in the Fig. 1: The proposed hybrid fault detection model for IoT networks combines the strengths of a Recurrent Neural Network (RNN) or Convolutional Neural Network (CNN) based model with a distrust model. These models work in parallel to analyze input data, produce feature vectors, and ultimately classify sensors into normal and anomaly categories. Here's a detailed step-by-step explanation of how this model operates:

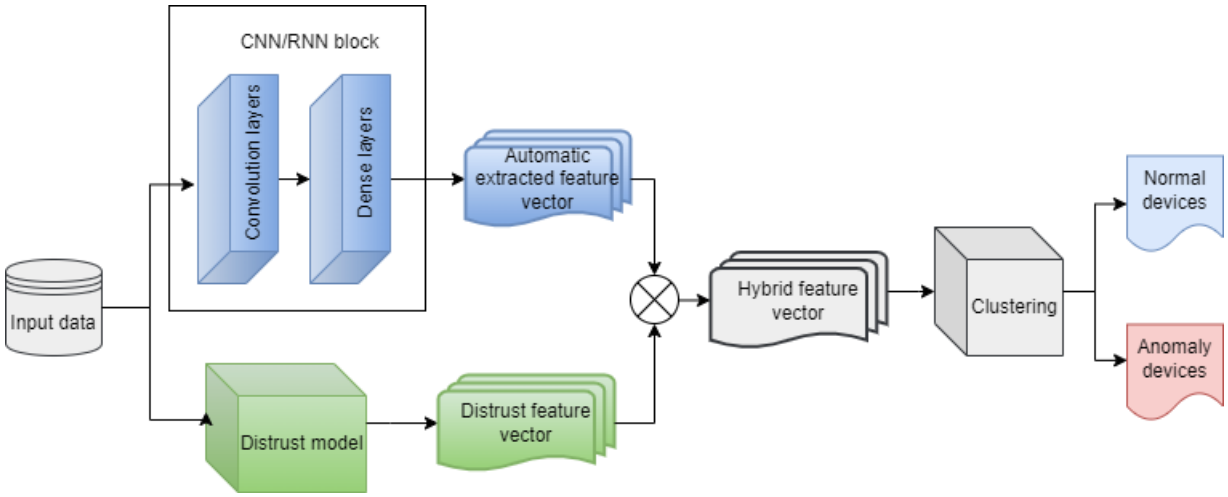

Figure 1: The combination of RNN and Distrust model

2.1 Data Collection and Pre-processing

- Input Data: The input data comprises the various metrics and signals collected from IoT sensors. This data can include sensor readings, sensor status logs, communication patterns, and other relevant parameters.
- Pre-processing: The raw data is pre-processed to remove noise, handle missing values, and normalize the values to ensure consistency and improve the model's performance.

2.2 Parallel Model Processing

2.2.1 Deep learning based model

The main idea in this work is do not use the full architect of a RNN/CNN model which may contain convolution layers, dense layers, and output (classification/prediction) layer. This model excludes the output layer from the architecture and uses only convolution and dense layers. Therefore, the output of this sub-system is feature vectors of input data. This feature vector is then merged with the feature from the distrust model before classifying (Fig. 1).

- Data Entry: The pre-processed data is fed into the RNN or CNN model.
- Feature Extraction: The RNN/CNN model outputs a feature vector, encapsulating the learned representations of the input data that highlight significant patterns and anomalies.

2.2.2 Distrust model

We make use these following notations in the model:

- There are n sensors in the network, noted from 1 to n.
- The value captured and sent to the management center by the sensor i, at the time t, is called s^t_i
- N is the set of nearest neighbor sensors of the sensor i.

This model is on the line with the work of Nguyen [14]. However, instead of estimating the value of distrust of each sensor, this model calculates the distrust vector of a sensor as follow:

- The difference between the sensor i to its neighbor j, at the time t is:

$$d^t_{ij} = | s^t_i - s^t_j | \quad (1)$$

- The distrust vector of sensor i regarding its neighbor j their difference during k-latest times:

$$V_{ij} = \{d_{ij}^{t-k+1}, d_{ij}^{t-k+2}, ..., d_{ij}^{t}\} \quad (2)$$

- The distrust vector of sensor i regarding all its neighbors is a merged vector of all V_{ij} :

$$V_i = \{V_{i0}, V_{i1}, ..., V_{iN}\} \quad (3)$$

In the experiment, the three-latest times (K=3) and the number of the nearest neighbors of a sensor is pre-selected as 5-neighbors (N=5), based on the experiments of Nguyen [14]. Therefore, the Vi is a vector of K*N = 15 elements.

2.3 Feature Vector Merging

- Combining Features: The feature vectors produced by the RNN/CNN-based model and the distrust model are concatenated to form a hybrid feature vector for each sensor. This vector combines the strengths of both models, incorporating both learned patterns and trust-based assessments.

2.4 Clustering and Classification

- Cluster Layer Input: The set of hybrid feature vectors for all sensors is input into a clustering layer.
- Clustering Process: The clustering layer, using an algorithm such as k-means or SVM (Support Vector Machine), processes the hybrid feature vectors to group them into clusters. This clustering separates sensors based on the similarities and differences in their hybrid feature representations.
- Subset Formation: The clustering layer produces two primary subsets:
  - Normal sensors Subset: sensors that exhibit normal, expected behavior and are deemed reliable.
  - Anomaly sensors Subset: sensors that display abnormal patterns or behaviors, indicating potential faults or reliability issues.

The hybrid model integrates RNN/CNN-based deep learning techniques with a distrust model to leverage both temporal/spatial pattern recognition and historical/contextual trust evaluation. By merging the output feature vectors from these models, the hybrid feature vectors provide a comprehensive representation of each sensor's status. The clustering layer then effectively classifies sensors into normal and anomaly categories, enabling efficient and accurate fault detection in IoT networks.

3. Evaluation

This section presents an experiment to evaluate the proposed model to some related models.

3.1 Dataset

This experiment uses the simulated data from the work of Nguyen [14], which is collected the AQI (EPA's index for reporting air quality - https://www.airnow.gov/aqi/aqi-basics/) from 340 sensors placed in the city of Hanoi during a year.

3.2 Baseline models

The chosen baseline models is based on their approach:

- The work which is based on the deep learning (Model 1): The are many models in this approach, one notable example is the work of Alghofaili and Rassam [2] which employs a combination of the simple multi-attribute rating technique (SMART) and long short-term memory (LSTM) algorithm; another example is the model Ali-Eldin [3] which uses a hybrid approach that combines a distributed computation technique and a global machine learning approach. For this experiment, the model by Alghofaili and Rassam [2] is selected as a representative deep learning-based model.
- The work which is based on a distrust model (Model 2): There are many proposed approaches such as the work of Macedo et al. [12], Nguyen [14], etc. In this study, we selected the model by Nguyen [14] for comparison, as its distrust model forms the basis of the distrust component in our proposed hybrid model.

By selecting these representative models, we aim to provide a comprehensive comparison of our proposed hybrid method against well-established approaches in both deep learning and distrust-based fault detection in IoT networks.

3.3 Scenario

Accordingly, the scenario for this experiment is as follow:

- Simulate the air pollution observation of the Hanoi city as in the work of Nguyen [14]: The faulty rate among sensors is fixed at 5%.
- Record the captured data for each sensor. And then, using it to apply the three considered models (Alghofaili and Rassam [2], Nguyen [14], and the ours) to detect the error sensors. In the model of Nguyen [14] and the distrust part of ours, the three-latest times (K=3) and 5-neighbors (N=5) is chosen based on the experiments of Nguyen [14].
- Repeat these above steps 20 times, and then, calculate the mean of output parameters (Accuracy, F1-score)

By following these steps, we aim to thoroughly evaluate the performance of the proposed hybrid model in comparison to the baseline models in detecting faulty sensors in a simulated air pollution monitoring scenario.

The considered output parameters are accuracy and F1-score. They are calculated based on the definition of Salton et al. [21]:

- Number of true positive (TP): This is the number of sensor which is good in the reality, and in the results, it is also concluded as trusted sensor.
- Number of false positive (FP): This is the number of sensor which is error in the reality, but in the results, it is concluded as trusted sensor.

- Number of false negative (FN): This is the number of sensor which good in the reality, but in the results, it is concluded as distrusted sensor.
- Number of true negative (TN): This is the number of sensor which is error in the reality, and in the results, it is also concluded as distrusted sensor.

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} * 100\% \quad (4)$$

$$Precision = \frac{TP}{TP+FP} * 100\% \quad (5)$$

$$Recall = \frac{TP}{TP+FN} * 100\% \quad (6)$$

$$F1-score = 2 * \frac{Precision*Recall}{Precision+Recall} \quad (7)$$

3.4 Results

The results are presented in the Fig.2. The proposed model achieves an accuracy of 99.53%. This performance is significantly higher compared to the accuracy of the model by Alghofaili and Rassam [2], which is 97.03%. The statistical significance of this improvement is confirmed with a *p-value* of less than 2e − 06. Additionally, the proposed model outperforms the model by Nguyen [14],which is 98.95%.The improvement in this case is also statistically significant, with a *p-value* of less than 0.016.

At the F1-score value, the proposed model achieves a value of 99.73%. This is significantly higher than the F1-score obtained by the model of Alghofaili and Rassam [2], which is 98.40%. The *p-value* for this comparison is less than 9e − 07, indicating strong statistical significance. The proposed model also surpasses the F1-score of Nguyen's model [14], which is 99.45%, with a *p-value* of less than 0.015.

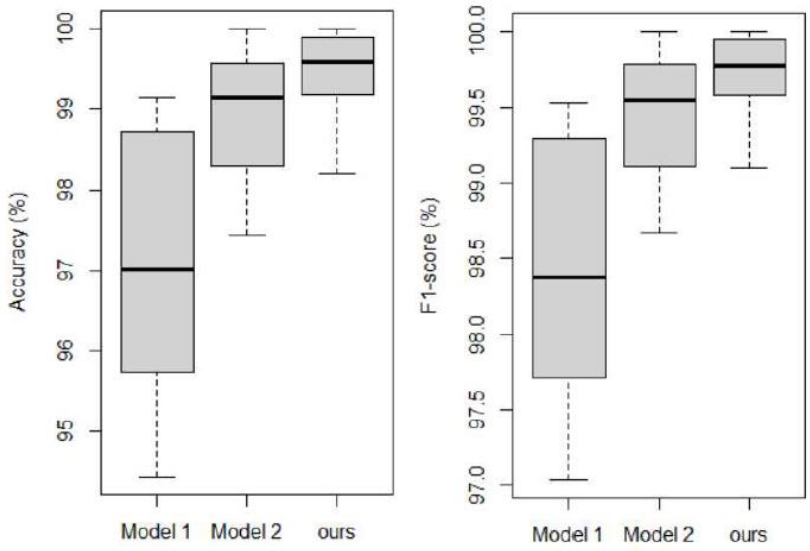

Figure 2: Comparison to some other works

In summary, the proposed model demonstrates significantly superior performance in both accuracy and F1-score compared to the two baseline models in the simulated system. These results underscore the effectiveness and robustness of the proposed hybrid method in detecting faulty sensors within an IoT network. By enhancing the accuracy of fault detection, this study offers a valuable solution for maintaining reliability in critical IoT applications such as smart cities, healthcare, and industrial automation.

4. Conclusion

Automatic detection of faulty sensors in an IoT network is crucial for maintaining the reliability, performance, security, and cost-effectiveness of the network. It supports scalability, ensures compliance, enhances user satisfaction, and enables proactive maintenance strategies. This study introduces a hybrid deep learning and distrust model for detecting faulty sensors in IoT networks, achieving high accuracy and reduced false positives. Our hybrid method leverages the strengths of deep learning to analyze complex data patterns and detect anomalies, while the distrust model evaluates sensor reliability based on historical and contextual data. Tested on simulated data from Hanoi's air pollution network, the model surpasses traditional techniques, underscoring its potential in enhancing IoT network reliability for various critical applications.

References

[1] Adel Abusitta, Glaucio H.S. de Carvalho, Omar Abdel Wahab, Talal Halabi, BenjaminC.M. Fung, and SajaAlMamoori. Deep learning-enabled anomaly detection for IoT systems. Internet of Things, 21:100656, 2023.

[2] Yara Alghofaili andMurad A. Rassam. A trust management model for IoT devices and services based on the multi-criteria decision-making approach and deep long short term memory technique. Sensors, 22(2), 2022.

[3] AmrM. T. Ali-Eldin. A hybrid trust computing approach for IoT using social similarity and machine learning. PLOS ONE, 17:1–28, 07 2022.

[4] Hussein Alsheakh and Shameek Bhattacharjee. Towards a unified trust framework for detecting IoT device attacks in smart homes. In 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pages 613–621, 2020.

[5] Ayan Chatterjee and Bestoun S. Ahmed. IoT anomaly detection methods and applications: A survey. Internet of Things, 19:100568, 2022.
[6] Abebe Abeshu Diro, Naveen Chilamkurti, Van-Doan Nguyen, and Will Heyne. A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms. Sensors, 21(24):13, 2021.
[7] Shangbin Han, Qianhong Wu, and Yang Yang. Machine learning for internet of things anomaly detection under low-quality data. International Journal of Distributed Sensor Networks, 18(10), 2022.
[8] Max Landauer, Sebastian Onder, Florian Skopik, and Markus Wurzenberger. Deep learning for anomaly detection in log data: A survey. Machine Learning with Applications, 12:100470, 2023.
[9] Zhaoyu Gu Lina Yao and Hao Wang. Integrated fault diagnosis and fault-tolerant control of nonlinear network control systems. International Journal of Innovative Computing, Information and Control, 16(4):1385–1398, 2020.
[10] Zhipeng Liu, Niraj Thapa, Addison Shaver, Kaushik Roy, Xiaohong Yuan, and Sajad Khorsandroo. Anomaly detection on iot network intrusion using machine learning. In 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD), pages 1–5, 2020.
[11] Wei Ma, Xing Wang, Mingsheng Hu, and Qinglei Zhou. Machine learning empowered trust evaluation method for IoT devices. IEEE Access, 9:65066–65077, 2021.
[12] Evandro Macedo, Flávia Delicato, Luís Moraes, and Giancarlo Fortino. A two-level integrated approach for assigning trust metrics to internet of things devices. Pages 26–36, 01 2022.
[13] Rim Magdich, Hanen Jemal, Chaima Nakti, and Mounir Ben Ayed. An efficient trust related attack detection model based on machine learning for social internet of things. In 2021 International Wireless Communications and Mobile Computing (IWCMC), pages 1465–1470, 2021.
[14] Manh Hung Nguyen. A distrust model to detect faulty sensor in an IoT network. In Proceedings of The 19th IEEE - RIVF International Conference on Computing and Communication Technology, pages 53–58, 12 2023.
[15] Manh Hung Nguyen and Dinh Que Tran. A combination trust model for multi-agent systems. International Journal of Innovative Computing, Information and Control, 9(6):2405–2420, 2013.
[16] Manh Hung Nguyen and Dinh Que Tran. A trust-based mechanism for avoiding liars in referring of reputation in multiagent system. International Journal of Advanced Research in Artificial Intelligence (IJARAI), 4(2):28–36, 2015.
[17] Manh Hung Nguyen and Dinh Que Tran. A trust model for new member in multiagent system. Vietnam Journal of Computer Science, 2(3):181–190, 2015.
[18] Guansong Pang, Chunhua Shen, Longbing Cao, and Anton Van Den Hengel. Deep learning for anomaly detection: A review. ACM Computing Surveys, 54(2):1-38, March 2021.
[19] K Prathapchandran and T Janani. A trust-based security model to detect misbehaving nodes in internet of things (IoT) environment using logistic regression. Journal of Physics: Conference Series, 1850(1):012–031, may 2021.
[20] Nilesh Kumar Sahu and Indrajit Mukherjee. Machine learning based anomaly detection for IoT network: (anomaly detection in IoT network). In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), pages 787–794, 2020.
[21] Gerard Salton and Michael J. McGill. Introduction to Modern Information Retrieval. McGraw-Hill, Inc., New York, NY, USA, 1986.
[22] Subarna Shakya. Process mining error detection for securing the IoT system. Journal of ISMAC, 2:147–153, 07 2020.
[23] Dinh Que Tran and Manh Hung Nguyen. Modeling trust in open distributed multiagent systems. East-West Journal of Mathematics, Special issue for Contribution in Mathematics and Applications III:98–108, 2010.
[24] Mohammed Zakariah and Abdulaziz S. Almazyad. Anomaly detection for IoT systems using active learning. Applied Sciences, 13(21), 2023.

Author Profile

Manh Hung Nguyen received B.E in Computer Science (CS) at PTIT in 2004, M.Sc. in CS at the Institute Francophone International (IFI) in 2007, and Ph.D in CS at the University of Toulouse, France, in 2010. He is currently working as an associate professor at the Faculty of Computer Science, at The Posts and Telecommunications Institute of Technologies (PTIT), Hanoi, Vietnam. His domains of interest are: Artificial Intelligence, Multi-agent system, Modeling and simulation of complex system, Machine learning.