

ELECTRICITY THEFT DETECTION WITH CONVOLUTIONAL NEURAL NETWORKS BASED ON SMART METERS DATA

Nguyen Quoc Minh*, Nguyen Dang Tien

School of Electrical and Electronic Engineering, Hanoi University of Science & Technology

ARTICLE INFO	ABSTRACT
Received: 06/5/2022	Electricity losses is one of the most important factor of the power quality. Electricity losses include technical and non-technical losses. Technical losses are caused by iron and copper losses in electric equipments such as generator, transmission line, transformer, motor. Non-technical losses, on the other hand, are normally caused by management problem, inaccurate metering data and electricity thief. In non-technical losses, electricity theft is the most popular type and account for high percent. However, this type of loss is very difficult to detect traditional methods. In this study, we propose to use deep learning method, based on a convolutional neural network model combined with a attention mechanism to detect electricity theft. The model was trained on the dataset collected from 42372 customers for 147 weeks. The dataset was obtained from China electricity utility company. The results show that the proposed model can detect the user's electricity theft with the AUC accuracy of 92.2%.
Revised: 31/5/2022	
Published: 31/5/2022	
KEYWORDS	
Electricity theft	
Smart grid	
Convolutional neural networks	
Deep learning	
Attention mechanism	

ỨNG DỤNG MẠNG NƠ-RON TÍCH CHẬP ĐỂ PHÁT HIỆN HÀNH VI ĂN TRỘM ĐIỆN DỰA TRÊN DỮ LIỆU TỪ CÔNG TƠ THÔNG MINH

Nguyễn Quốc Minh*, Nguyễn Đăng Tiến

Trường Điện - Điện tử, Trường Đại học Bách Khoa Hà Nội

THÔNG TIN BÀI BÁO	TÓM TẮT
Ngày nhận bài: 06/5/2022	Tổn thất điện năng là một trong các chỉ tiêu quan trọng để đánh giá chất lượng điện năng. Tổn thất điện năng bao gồm hai thành phần là tổn thất kỹ thuật và tổn thất phi kỹ thuật. Tổn thất kỹ thuật là tổn thất đồng và tổn thất sắt trên các thiết bị điện như máy phát điện, đường dây, máy biến áp, động cơ. Tổn thất phi kỹ thuật là tổn thất ở khâu quản lý, đo đếm điện năng và ăn trộm điện. Trong các loại tổn thất phi kỹ thuật, tổn thất điện năng do hành vi trộm cắp điện là dạng tổn thất phổ biến, gây thiệt hại về mặt kinh tế nhưng lại khó phát hiện bằng các phương pháp truyền thống. Trong nghiên cứu này, chúng tôi đề xuất sử dụng phương pháp học sâu, dựa trên mô hình mạng nơ-ron tích chập kết hợp với cơ chế tập trung để phát hiện hành vi trộm cắp điện. Mô hình được huấn luyện trên tập dữ liệu được thu thập từ 42372 khách hàng trong 147 tuần. Kết quả phân loại cho thấy, mô hình đề xuất có thể phát hiện được hành vi trộm cắp điện của người dùng với độ chính xác AUC là 92,2%.
Ngày hoàn thiện: 31/5/2022	
Ngày đăng: 31/5/2022	
TỪ KHÓA	
Trộm cắp điện	
Lưới điện thông minh	
Mạng nơ-ron tích chập	
Học sâu	
Cơ chế tập trung	

DOI: <https://doi.org/10.34238/tnu-jst.5947>

* Corresponding author. Email: minh.nguyenquoc@hust.edu.vn

1. Giới thiệu

Ngày nay, điện năng đã trở thành một trong những loại năng lượng thiết yếu nhất trong cuộc sống của chúng ta. Theo Ngân hàng thế giới, trong năm 2017, hơn 88% dân số thế giới được tiếp cận và sử dụng năng lượng điện được cung cấp thông qua một hệ thống lưới điện truyền tải từ nhà máy điện tới người tiêu dùng. Lưới điện thông minh đã trở thành một giải pháp quan trọng trong việc vận hành và giám sát năng lượng. Nó cung cấp cho khách hàng khả năng theo dõi, kiểm tra và dự đoán mức độ sử dụng điện năng bằng cách tích hợp các thiết bị kỹ thuật số hiện đại có thể thu thập các thông số của hệ thống điện qua giao thức truyền thông không dây, hệ thống Internet vạn vật (IoT).

Tuy nhiên, bên cạnh sự phát triển tích cực của nó, vẫn còn tồn tại nhiều hạn chế khó khăn chưa khắc phục được; đặc biệt là sự thiệt hại do tổn thất điện xảy ra trong quá trình phát điện, truyền tải và phân phối điện năng. Các biện pháp làm tăng hiệu quả trong quá trình tạo, truyền tải và phân phối điện là một bài toán nan giải không chỉ ở trong nước mà còn là trên khắp thế giới. Tổn thất điện năng thường được phân loại thành hai dạng chính là tổn thất kỹ thuật (TTKT) và tổn thất phi kỹ thuật (TTPKT). Tổn thất kỹ thuật xảy ra do tản điện trong các vật liệu tạo nên hệ thống điện, chẳng hạn như cáp, đầu nối và máy biến áp điện. Tổn thất phi kỹ thuật đại diện cho tổn thất năng lượng do trộm cắp và sai sót khi lập hoá đơn hoặc đo lường [1].

Trong nghiên cứu này, chúng tôi tập trung nghiên cứu về tổn thất phi kỹ thuật do hành vi trộm cắp điện gây nên. Các hành vi sai trái này thường được thực hiện bằng việc đưa điện năng không thông qua đồng hồ đo, hoặc làm cho đồng hồ không thực hiện được đúng chức năng. Theo Báo cáo tổn thất phân phối điện được công bố bởi ANEEL (Cơ quan Điện lực Quốc gia Brazil) [2], tổn thất điện phi kỹ thuật chiếm khoảng 6,6% tổng năng lượng được đưa vào hệ thống điện Brazil vào năm 2018. Ngay cả một cường quốc như Hoa Kỳ thì thiệt hại do trộm cắp điện được ước tính vào khoảng 4,5 tỷ đô la mỗi năm [3]. Theo báo cáo [4] năm 2020, công ty Điện lực Hà Tĩnh đã phát hiện, xử lý 92 vụ trộm cắp điện, truy thu 188.449 kWh điện, tương đương trên 603 triệu đồng.

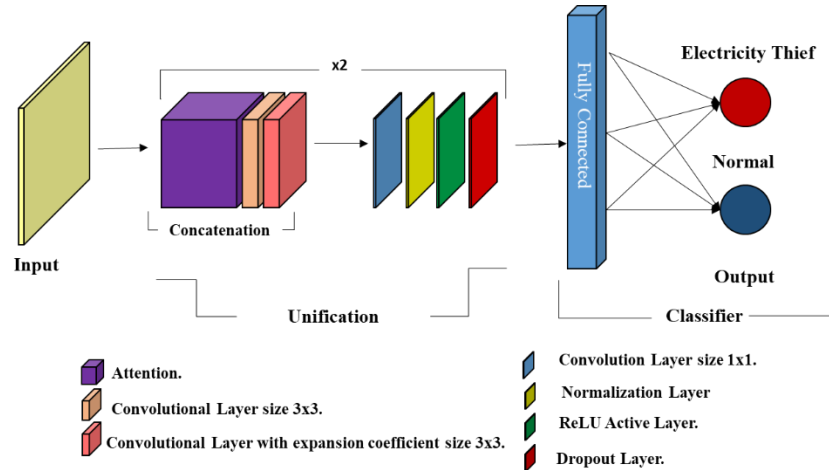
Do đó, trộm cắp điện là vấn đề chung trên toàn thế giới và đã có rất nhiều những nghiên cứu trước đây nhằm đưa ra các phương pháp để giải quyết vấn đề này. Các phương pháp phát hiện trộm cắp điện thông thường bao gồm: kiểm tra việc lắp đặt, sử dụng và tình trạng hoạt động của đồng hồ, so sánh các chỉ số đo bất thường với những cái bình thường và kiểm tra đường truyền... Tuy nhiên, các phương pháp này vô cùng tốn thời gian, cần một nguồn nhân lực lớn, tốn kém về tài chính nhưng không mang lại nhiều hiệu quả. Cũng có một số phương pháp tiên tiến hơn như: Sử dụng lưới điện thông minh [5], thuật toán vector hỗ trợ (SVM) [6], rừng ngẫu nhiên [7], mạng nơ-ron nhân tạo [8] để phát hiện trộm cắp điện. Tuy nhiên, các phương pháp đó có độ chính xác thấp vì hầu hết dữ liệu được sử dụng theo 1 chiều (1-D) và không thể nắm bắt chu kỳ tiêu thụ điện của người tiêu dùng.

Tại nghiên cứu này, chúng tôi đề xuất sử dụng một phương pháp học có giám sát dựa trên các mạng nơ-ron tích chập (Convolutional Neural Network - CNN) kết hợp với cơ chế tập trung (Self-attention) để nhận dạng và phát hiện các hành vi trộm cắp điện của người tiêu dùng. Đây là một phương pháp giúp tiết kiệm chi phí, thời gian và ngân sách của nhà cung cấp điện.

2. Mô hình phát hiện trộm cắp điện sử dụng mạng nơ-ron tích chập

Tính hiệu quả và ưu việt của cơ chế tập trung đã được khẳng định và chứng minh thông qua các bài toán thuộc lớp xử lý ngôn ngữ tự nhiên. Trong các nghiên cứu gần đây, cơ chế tập trung cũng được sử dụng cho các lớp bài toán thị giác máy, dữ liệu dạng bảng cho kết quả khả quan. Tại nghiên cứu này, chúng tôi cũng đề xuất mô hình kết hợp sử dụng cơ chế tập trung và các lớp tích chập, chi tiết mô hình được thể hiện như *Hình 1* dưới đây.

Lớp tích chập: Mô hình đề xuất sử dụng lớp tích chập gồm hai phần. Cụ thể phần đầu tiên là lớp tích chập tiêu chuẩn có kích thước nhân 3x3, phần còn lại là lớp tích chập với hệ số giãn nở là 2, kích thước nhân 3x3. Kết quả của hai phần sẽ được nối lại để tạo thành một đầu ra duy nhất cho lớp.



Hình 1. Kiến trúc mô hình đề xuất sử dụng kết hợp cơ chế tập trung và các lớp tích chập

Cơ chế tập trung: Trong mô hình này, cơ chế tập trung đề xuất sẽ sử dụng các kênh của đầu vào làm các đầu của cơ chế tập trung. Đầu tiên, với đầu vào 3 chiều có kích thước (C, L, D) sẽ được trải phẳng và biến đổi thành ma trận 2 chiều $X \in \mathbb{R}^{C \times LD}$, giúp cho ma trận trọng số $W_q, W_k, W_v \in \mathbb{R}^{CD \times \bar{C}D}$ có thể biểu diễn được mối quan hệ. Trong đó, C số kênh của đầu vào hay số đầu vào của cơ chế tập trung, L là kích thước độ dài chuỗi đầu vào, D số lượng các chuỗi của đầu vào, $\bar{C}$ là số kênh của đầu ra hay số đầu ra của cơ chế tập trung. Khi đó từng đầu ra sẽ được tính $O_{q,k,v} = XW_{q,k,v}$, $O_{q,k,v} \in \mathbb{R}^{L \times \bar{C}D}$, kế tiếp sẽ biến đổi và chuyển vị lại thành 3 chiều $\bar{O}_{q,k,v} \in \mathbb{R}^{\bar{C} \times L \times D}$, cuối cùng sẽ được đi qua lớp *Softmax* theo công thức (1), điều này cho phép nhất quán về kích thước để kết hợp với lớp tích chập.

$$Attn = \text{Softmax} \left(\frac{\bar{O}_q \bar{O}_k^T}{\sqrt{D}} \right) \bar{O}_v \quad (1)$$

Trích xuất đặc trưng: Sau khi đầu vào được đi qua khối cơ chế tập trung kết hợp với lớp tích chập, sẽ được cho qua một lớp tích chập khác có kích thước nhân là 1×1 , có nhiệm vụ thống nhất lại đặc trưng, theo sau là các lớp chuẩn hóa, lớp kích hoạt và lớp dropout.

Phân loại: Cuối cùng, đầu ra của các lớp trước đó được trải phẳng và đưa vào một mạng nơ-ron truyền thẳng kết nối đầy đủ, đầu ra phân loại là người dùng có hành vi ăn cắp điện hoặc là bình thường.

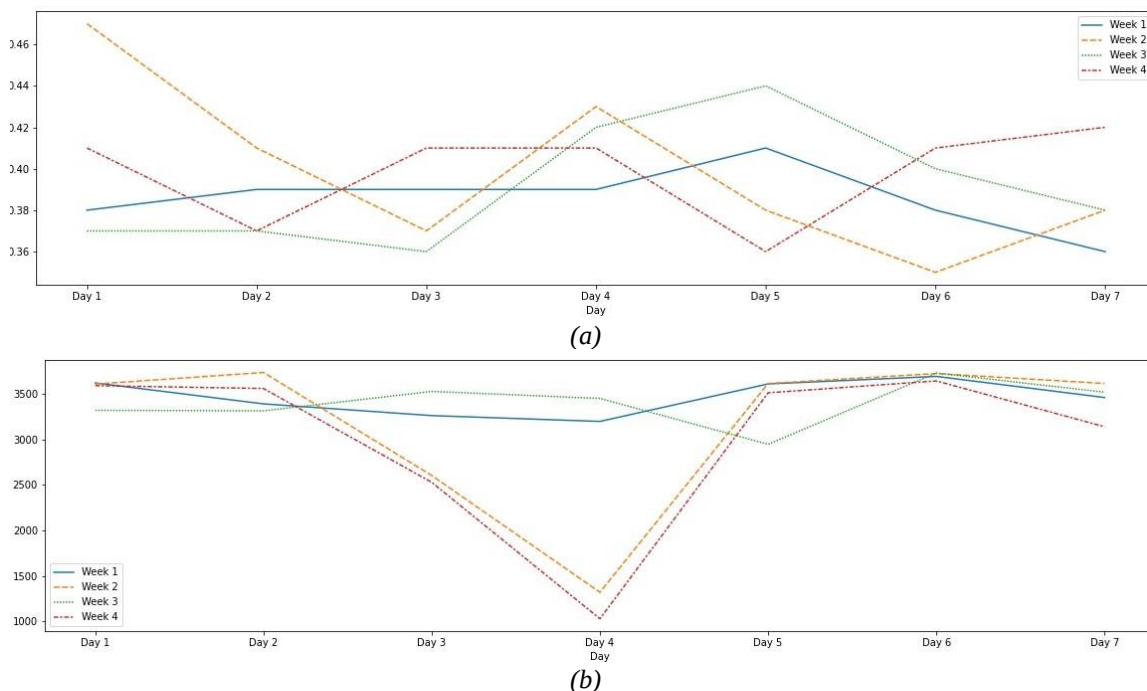
Trong kiến trúc mô hình của mình, chúng tôi sử dụng hai lần khối trích xuất đặc trưng, với khối đầu tiên số đầu của cơ chế tập trung $C = 2$, số đầu ra $\bar{C} = 16$, khối thứ hai $C = 48$, $\bar{C} = 16$. Phần lớp tích chập sẽ nhận đầu vào là 2 kênh ma trận 2D, đầu ra 32 kênh với ma trận có cùng kích thước, số bộ lọc được sử dụng ở các lớp tích chập lần lượt là 16 tại lớp tích chập tiêu chuẩn và 16 tại lớp tích chập có hệ số giãn nở. Tại mạng kết nối đầy đủ, chúng tôi dùng 1024 nơ-ron cho lớp ẩn và lớp đầu ra gồm 2 nơ-ron.

Mô hình được huấn luyện và kiểm thử trên bộ dữ liệu được thu thập và công bố bởi Tổng công ty lưới điện Trung Quốc (State Grid Corporation of China). Bộ dữ liệu bao gồm mức tiêu thụ điện năng hàng ngày của 42372 khách hàng được thu thập thông qua các công tơ mét thông minh. Dữ liệu được thu thập từ ngày 01/01/2014 tới ngày 31/10/2016, tương ứng với khoảng 147 tuần. Dữ liệu được gán nhãn thành hai loại là người dùng điện thông thường và người dùng điện có hành vi trộm cắp, dữ liệu không thể hiện ngày hành vi trộm cắp được thực hiện. Trong đó, tỉ lệ nhãn là người dùng trộm cắp điện chiếm xấp xỉ 8,53%; tỉ lệ dữ liệu bị thiếu chiếm gần 25,64%. Chi tiết về tập dữ liệu được thể hiện tại *Bảng 1*.

Bảng 1. Mô tả tập dữ liệu của Tổng công ty lưới điện Trung Quốc.

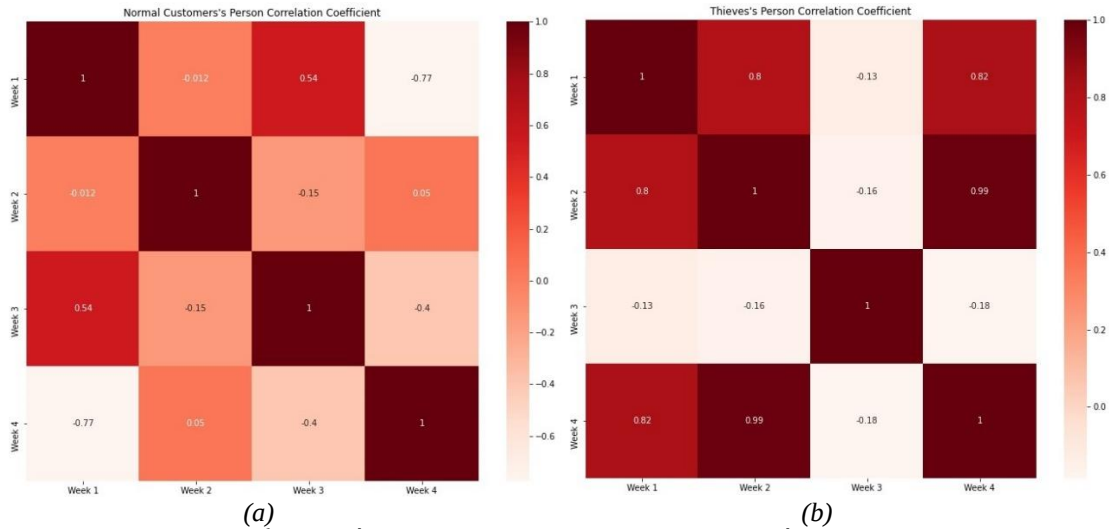
Mô tả	Giá trị
Thời gian thu thập dữ liệu	01/01/2014 – 31/10/2016
Tổng số khách hàng	42 372
Khách hàng bình thường	38 757 (91,47%)
Khách hàng trộm cắp điện	3 615 (8,53%)

Trong nghiên cứu này, chúng tôi nhận thấy rằng có sự biến động về lượng điện tiêu thụ theo từng ngày của khách hàng, sự biến động này lớn hơn tại các khách hàng được gán nhãn là ăn cắp điện. Các đặc trưng này rất khó thể hiện được dưới dạng dữ liệu 1-D, tuy nhiên với cách định hình dữ liệu thành 2-D theo tuần thì có thể dễ dàng nhận thấy chu kỳ tiêu thụ điện của khách hàng như Hình 2. Trong đó tại dữ liệu tiêu thụ điện của khách hàng bình thường, không có dấu hiệu bất thường, dao động trong một khoảng hẹp. Tuy nhiên, với dữ liệu sử dụng điện của khách hàng được gán nhãn là trộm cắp điện có thể nhận thấy điện năng tiêu thụ sụt giảm lớn tại ngày thứ 4 của tuần 2 và tuần 4.



Hình 2. (a) Tính chu kỳ điện năng của khách hàng bình thường thông qua các tuần và (b) Sự bất thường trong chu kỳ tiêu thụ điện năng của khách hàng ăn trộm điện qua các tuần

Để thể hiện rõ ràng hơn tính chu kỳ tiêu thụ điện của người dùng bình thường và sự bất bình thường trong hành vi tiêu thụ điện của người dùng trộm cắp điện, chúng tôi thực hiện phân tích mối tương quan trên dữ liệu tiêu thụ điện. Tại Hình 3 cho thấy ma trận hệ số tương quan của cả khách hàng bình thường và trộm cắp điện năng theo tuần. Cụ thể, tại Hình 3a) thể hiện giá trị tương quan phụ tải tiêu thụ của khách hàng bình thường, trong khi Hình 3b) thể hiện mối tương quan phụ tải của khách hàng ăn trộm điện. Với mối tương quan tiêu thụ điện năng giữa các tuần của khách hàng bình thường ta có thể nhận thấy không có sự bất thường, tuy nhiên mối tương quan tiêu thụ điện năng của khách hàng trộm cắp điện cho thấy sự thay đổi lớn tại các tuần ghi nhận sự biến động sụt giảm điện năng tiêu thụ.



Hình 3. (a) Ma trận thể hiện mối tương quan tiêu thụ điện năng theo tuần của khách hàng bình thường và (b) Ma trận thể hiện mối tương quan tiêu thụ điện năng theo tuần của khách hàng có hành vi trộm cắp điện

Mô hình được xây dựng bằng ngôn ngữ lập trình python, sử dụng thư viện Pytorch và huấn luyện trên GPU NVIDIA Tesla T4. Nghiên cứu được huấn luyện theo kỹ thuật kiểm định chéo K-fold, với giá trị $k = 5$ được khởi tạo. Trong nghiên cứu này, chúng tôi sử dụng phương pháp tối ưu hoá mạng nơ-ron RAdam, độ hiệu quả của phương pháp được chứng minh và thực nghiệm cho thấy cải thiện so với các phương pháp trước đó như Adam, SGD [9].

3. Kết quả và bàn luận

Trong nghiên cứu này, để kiểm tra kết quả phân loại của mô hình chúng tôi sử dụng chỉ số diện tích dưới đường cong ROC (AUC) để đánh giá. ROC (Receiver operating characteristic) là một đường cong biểu diễn xác suất và AUC (Area under the ROC Curve) biểu diễn mức độ phân loại trung bình của mô hình. AUC thể hiện xác suất một mẫu dương tính được lấy ngẫu nhiên xếp hạng cao hơn một mẫu âm tính được lấy ngẫu nhiên, được thể hiện tại công thức (4). Đường cong ROC biểu diễn các cặp chỉ số (*Recall*, *FPR*) tại mỗi ngưỡng với *Recall* (*TPR*) ở trục tung và *FPR* ở trục hoành. Chúng tôi cũng dựa trên chỉ số F1-Score để đánh giá hiệu suất và dùng làm tiêu chuẩn để tinh chỉnh các tham số mô hình. Công thức của chỉ số đánh giá F1-Score được thể hiện tại (6). Ngoài ra chúng tôi còn sử dụng độ chính xác trung bình MAP [10] để đo lường độ hiệu quả của việc đưa ra kết quả dự báo.

$$Recall = \frac{TP}{TP + FN} \quad (2)$$

$$FPR = \frac{FP}{TN + FP} \quad (3)$$

$$AUC = P(score(x^+) > score(x^-)) \quad (4)$$

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

$$F1 = 2 * \frac{Precision * Recall}{Precision + Recall} = \frac{2TP}{TP + FP + FN} \quad (6)$$

$$MAP@K = \frac{1}{\sum_{i=1}^K r_i} \sum_{i=1}^K r_i \left(\frac{\sum_{j=1}^i r_j}{i} \right) \quad (7)$$

Trong đó, *TP* là số lượng mô hình dự đoán khách hàng ăn trộm điện là đúng, *TN* là số lượng mô hình dự đoán khách hàng bình thường là đúng, *FP* là số lượng mô hình dự đoán khách hàng ăn trộm điện là sai, *FN* là số dự đoán của mô hình cho ra kết quả khách hàng bình thường là sai. Để

tính giá trị MAP, trước tiên cần sắp xếp các giá trị nhân thực tế theo xác suất mô hình dự đoán, lấy K giá trị đầu và tính theo công thức (7), với r_i là giá trị nhân thực tế của khách hàng thứ i , $r_i = 1$ nếu là khách hàng trộm có hành vi trộm cắp và $r_i = 0$ khi là khách hàng bình thường.

Chúng tôi đã đánh giá mô hình trên tập kiểm thử đã được chia và cách ly khỏi tập huấn luyện với tỉ lệ 80-20.

Bảng 2. Kết quả của mô hình trên tập kiểm thử

Chỉ số	%
AUC	92,2
MAP@100	99,2
MAP@200	98,2
F1-Score	64,5

Bảng 3. So sánh mô hình đề xuất với các nghiên cứu khác trên cùng tập dữ liệu

Chỉ số	AUC (%)	F1-Score (%)
AdaBoost[11]	53,46	13,34
DANN[11]	69,00	45,83
CNN[12]	78,15	-
Mô hình đề xuất	92,2	64,5

Tại *Bảng 2*, chúng tôi đã trình bày độ chính xác của mô hình đề xuất. Có thể thấy độ chính xác AUC đạt được là 92,2%, MAP@100 là 99,2%, MAP@200 là 98,2%. Chúng tôi cũng so sánh với những mô hình khác được huấn luyện và kiểm thử trên cùng bộ dữ liệu của Tổng công ty lưới điện Trung Quốc tại *Bảng 3*, kết quả cho thấy các mô hình học máy như AdaBoost được Bohani và các cộng sự [11] huấn luyện cho kết quả tương đối thấp chỉ đạt AUC 53,46%, F1-Score 13,34%. Cũng tại nghiên cứu đó kết quả của mạng nơ-ron sâu cho thấy đây là một hướng khả quan khi AUC được cải thiện lên 69%, F1-Score 45,85%. Tuy nhiên, mạng nơ-ron đơn thuần là không đủ, Zheng và các cộng sự [12] đã cải thiện độ chính xác AUC 78,15% khi sử dụng mạng nơ-ron tích chập. Với việc sử dụng cơ chế tập trung trong mạng nơ-ron tích chập, nhóm nghiên cứu đã cải thiện một cách đáng kể. Tuy nhiên, do sự mất cân bằng về dữ liệu giữa các khách hàng được gán nhãn là có hành vi ăn trộm điện và khách hàng bình thường, kết hợp với việc dữ liệu bị khuyết với tỉ lệ 25,64% khiến cho mô hình gặp nhiều khó khăn trong việc xác định được hành vi trộm cắp, chỉ số F1-Score đạt được là 64,5%. Nghiên cứu này mở ra nhiều hướng nghiên cứu để cải thiện độ chính xác trong tương lai.

4. Kết luận

Nghiên cứu này đề xuất một cách tiếp cận để phát hiện tự động các hành vi trộm cắp điện trong lưới điện thông minh dựa trên mô hình tích chập kết hợp với cơ chế tập trung. Từ kết quả nghiên cứu đã chỉ ra rằng, mô hình mạng nơ-ron đề xuất cho kết quả khả quan với độ chính xác AUC là 92,2% vượt trội so với các thuật toán học máy, mạng nơ-ron đơn giản. Trong tương lai, nhóm sẽ tiếp tục nghiên cứu cải thiện mô hình học sâu để nâng cao độ chính xác của thuật toán.

TÀI LIỆU THAM KHẢO/ REFERENCES

- [1] P. Glauner *et al.*, "The challenge of non-technical loss detection using artificial intelligence: A survey," *International Journal of Computational Intelligence Systems*, vol. 10, no. 1, p. 760, 2017.
- [2] ANEEL, "Perdas de energia eltrica na distribuio," 2019. [Online]. Available: <http://www.aneel.gov.br/documents/654800/18766993/Relatrio+Perdas+de+Energia +Edio+1-2019-02-07.pdf>, 07.2019.
- [3] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy Magazine*, vol. 7, no. 3, pp. 75-77, 2009.
- [4] PC Ha Tinh, "Detect 92 electricity theft from customers with 600 millions VND fine," 2021. [Online]. Available: <https://thuonghieucongluan.com.vn/dien-luc-ha-tinh-xu-ly-92-vu-an-cap-dien-truy-thu-hon-600-trieu-dong-a125633.html>, 01.2021.

-
- [5] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1319-1330, 2013.
 - [6] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Inform.*, vol. 12, pp. 1005-1016, 2016.
 - [7] S. Li, Y. Han, X. Yao, S. Yingchen, J. Wang, and Q. Zhao. "Electricity Theft Detection in Power Grids with Deep Learning and Random Forests," *Journal of Electrical and Computer Engineering*, vol. 2019, 2019, Art. no. 4136874.
 - [8] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and P. Nelapati, "A hybrid neural network model and encoding technique for enhanced classification of energy consumption data," Proceedings of the 2011 IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 24–29 July 2011.
 - [9] L. Liu, H. Jiang, P. He, W. Chen, X. Liu, J. Gao, and J. Han, "On the variance of the adaptive learning rate and beyond," The International Conference on Learning Representations, 2020.
 - [10] A. Turpin and F. Scholer, "User performance versus precision measures for simple search tasks," Proceedings of the 29th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, SIGIR 06, New York, NY, USA, 2006.
 - [11] F. A. Bohani, A. Suliman, M. Saripuddin, S. S. Sameon, N. S. Md Salleh, and S. Nazeri, "A Comprehensive Analysis of Supervised Learning Techniques for Electricity Theft Detection," *Journal of Electrical and Computer Engineering*, vol. 2021, 2021, Art. no. 9136206.
 - [12] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, "Wide & Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1606-1615, April 2018.