A CNN-BASED MODEL FOR DETECTING WEBSITE DEFACEMENTS

Hoang Xuan Dau[*], **Nguyen Trong Hung**[+]

[*] Posts and Telecommunications Institute of Technology
[+] Academy of People's Security

Abstract— Over last decade, defacement attacks to websites and web applications have been considered a critical threat in many private and public organizations. A defacement attack can result in a severe effect to the owner's website, such as instant discontinuity of website operations and damage of the owner's fame, which in turn may lead to big financial damages. Many solutions have been studied and deployed for monitoring and detecting defacement attacks, such as those based on simple comparison methods and those based on complicated methods. However, some solutions only work on static web-pages and some others can work on dynamic web-pages, but they generate high level of false alarms. This paper proposes a Convolutional Neural Network (CNN)-based detection model for website defacements. The model is an extension of previous models based on traditional supervised machine learning techniques and its aims are to improve the detection rate and reduce the false alarm rate. Experiments conducted on the dataset of 100,000 web-pages show that the proposed model performs significantly better than models based on traditional supervised machine learning.

Keywords— CNN-based Model for Defacement Detection, Defacement Attacks to Website, Detection of Website Defacements.

I. INTRODUCTION

Defacements to websites and web applications are a class of web attacks, which amend the web content and thus change their appearance [1][2]. Fig. 1 is the website of UK National Health Services (NHS), which was defaced in 2018 with the message "*Hacked by AnoaGhost – Typical Idiot Security*" left on the website [1]. It is reported that the NHS website may have been defaced for as long as 5 days. In 2019, 15,000 websites of government organizations, banks, press agencies and television broadcasters in Georgia, a small European country, were defaced and took offline [1]. According to a recent report, the number of defacement attacks to websites globally has been risen sharply during the coronavirus lockdown with an increase of about 51% and 65% in April and May of 2020 compared to the figures of the same months of 2019, respectively [3]. Fig. 2 is a website of a UK-based canoe and kayak club was recently defaced in 2020 [3].

A number of reasons that websites and web applications were defaced have been pointed out. Among them, the prime reason is severe security vulnerabilities existed in websites, web applications, or hosting servers allow attackers to download files to the servers, or to have accesses to the websites' administrative pages. Common website vulnerabilities include XSS (Cross-Site Scripting), SQLi (SQL injection), file inclusion, inappropriate account and password administration, and no-update software [1][2].

Fig. 1. The UK NHS website was defaced in 2018 [1]

Fig. 2. A website of a U.K.-based canoe and kayak club was recently defaced [3]

Defacement attacks to websites can cause serious damages to their owners. The attacks can cause instant discontinuance to the normal operations of websites, harm

Contact: Hoang Xuan Dau,
Email: dauhx@ptit.edu.vn
Received: 04/1/2021, Revised: 27/2/2021, Accepted: 08/3/2021.

the reputation of website owners and lead to possible data leakages. These in turn may result in large financial losses [1][2]. Because of the wide spreading of defacement attacks and their serious consequences, many defensive measures have been researched and deployed in practice. Current defensive measures to defacement attacks can be classified into 3 main groups: (1) scanning and fixing website security vulnerabilities; (2) using website defacement monitoring and detecting tools, such as Nagios Web Application Monitoring Software [4], Site24x7 Website Defacement Monitoring [5] and WebOrion Defacement Monitor [6]; and (3) using various methods to detect website defacement attacks.

This paper proposes a detection model for website defacements, which is based on the Convolutional Neural Network (CNN). The proposed CNN-based model is an alternative approach of the traditional machine learning-based model proposed in [11], in which we exploit the power of the CNN-based text classification scheme to solve the problem of website defacement detection. In the proposed model, CNN learning is used to construct the model from the training data and then the model is used to classify monitored web-pages into either Normal or Defaced class.

The remaining of this paper is structured as follows: Section II discusses some closely related works; Section III describes our proposed model; Section IV shows experiments and results, and Section V is the paper conclusion.

II. RELATED WORKS

There have been some proposed techniques and tools for monitoring and detecting defacement attacks on websites and web applications. However, due to the paper scope, this section provides a review of some typical approaches that belong to group (3) mentioned in Section I. The proposed approaches of group (3) are composed of traditional methods and complicated or advanced methods. These methods will be discussed in the next sub-sections.

A. Traditional Methods for Detecting Defacements

Traditional methods for website defacement detection include checksum comparison, diff comparison and DOM tree analysis. The checksum comparison is the simplest technique to detect changes in web-pages. Firstly, the web page content's checksum is calculated using a hashing algorithm, such as MD5 or SHA1 and saved to the detection profile. Then, the web page is monitored and the new checksum is computed, and then compared with its checksum stored in the detection profile. If the two checksums are different, a defacement alarm is raised. This technique works well for static web-pages. For dynamic web-pages, such as e-commerce, or forum web-pages, it is not applicable because their content changes frequently [11][12][13].

In the Diff comparison method, the DIFF tool is used, which is popularly supported on Linux and UNIX systems to find the difference between two web-pages' content. The most difficult thing to do is to determine an anomaly threshold as the input for the monitoring process of each web-page. This technique is relatively effective and works well for dynamic websites if the anomaly detection threshold is determined properly [11][12][13].

Document Object Model (DOM) is an Application Programming Interface (API) that defines the logical structure of HTML documents, or web-pages. DOM can be used to scan and analyze the structure of the web-page. DOM tree analysis technique is used to detect changes in the page structure, rather than changes in the page content. Firstly, the page structure is extracted from the page content in the normal working condition and stored in the detection profile. Then, the page structure of the monitored page is extracted and then compared with the stored page structure saved in detection profile to find the difference. If a significant difference between the structures of two pages is found a defacement attack alarm is raised. Generally, this method works fine for web-pages with stable structures. However, this method is not able to detect unauthorized modifications in the web-pages' content [11][12][13].

B. Complicated Methods for Detecting Defacements

Complicated methods for detecting website defacements consist of those based on statistics [7], genetic programming [8][9], page screenshot analysis [10] and supervised machine leaning [11][12][13]. Kim et al. [7] proposed a statistical model based on 2-gram technique to construct a profile from normal web-pages for monitoring and detecting defacements, as shown in Fig. 3. Each normal web-page of the training set is converted to a vector, in which the page's HTML content is splitted to substrings using the 2-gram method and substrings' occurrence frequencies are counted. The detection profile is composed of vectors of all normal pages of the training set. Then, each monitored web-page is also converted to a vector and then its vector is compared with the page's vector stored in the profile to find the difference using the cosine distance. If the difference is greater than a threshold an alarm is raised. The paper also proposed an algorithm to generate a dynamic threshold for each web-page to reduce the false alarms. The proposed method's major shortcoming is for monitored pages with frequent changed content, the periodically adjusted thresholds are not appropriate and therefore the method still generates a high level of false alarms.

Bartoli et al. [8] and Davanzo et al. [9] proposed to use genetic programming to construct the detection profile for defacement attacks. In their approaches, information from monitored web-pages is monitored and extracted using 43 sensors embedded in web-pages. Each web-page's information is then converted into a 1466-element vector. In the training stage, normal web-pages are collected and vectorized to construct the profile based on genetic programming. In the detection stage, the monitored page is collected, vectorized and compared with the profile to look for the difference. Their approaches' the major drawback is it requires extensive computing resources for the detection profile construction since very large-size page vectors and slowly-converged genetic programming are used.

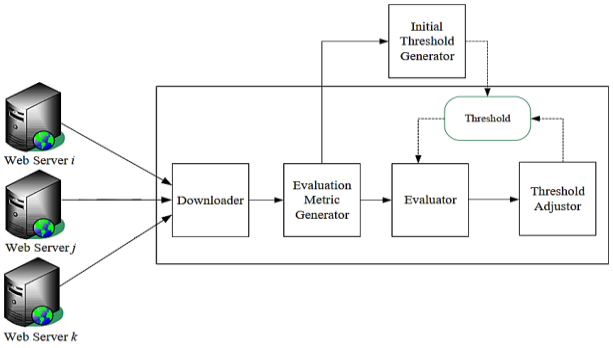


Fig. 3. Detection process for web page defacements proposed by Kim et. al. [7]

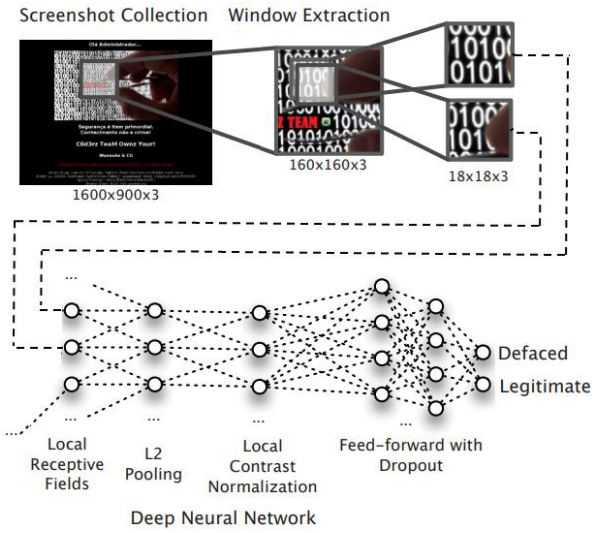


Fig. 4. Meerkat's architecture based on deep neural network [10]

Borgolte et al. [10] proposed Meerkat shown in Fig. 4, which is a system based on image object recognition of web-page screenshots using computer vision techniques for detecting defacement attacks. The system first builds a profile of screenshots of normal web-pages. It then takes the monitored web-page's screenshot and conducts analysis to find the difference between the page's current screenshot and its normal screenshots stored in the profile based on high-level screenshot features using advanced learning methods, such as stacked auto-encoder and deep neural network. Experiments con-ducted on 10 million of defaced web-pages and 2.5 million of normal web-pages show that the system achieves high detection accuracy from 97.422% to 98.816% and low false positive rate from 0.547% to 1.528%. The Meerkat's advantages are the profile can be constructed automatically and the system was tested on a large dataset. However, its major disadvantage is it requires extensively computational resources for highly complex image processing and recognition.

Hoang et al. [11][12][13] proposed several models for detecting website defacements, including the machine learning-based model, the hybrid model and the multi-layer model. The main idea behind these models is they use traditional supervised machine learning algorithms, such as naive bayes, decision tree and random forest to construct the detection models. Specifically, the problem of defacement detection is transferred to the text classification problem of web-pages' HTML content. The used dataset for training to build the detection model is a combination of normal web-pages and defaced web-pages. The detection model is then used to classify monitored web-pages into either Normal or Attacked class. The approach's strong points are (1) the detection model can be built automatically from the training data and (2) the overall detection accuracy is high. However, the approach's main drawbacks include (1) the false positive and negative rates are still relatively high and (2) the experimental datasets of only about 1000-3000 web-pages are relatively small in order to get a high level of reliability of the reported results.

In this paper, we extend the defacement detection model proposed in [11][12][13] by using CNN – a deep machine learning method, instead of traditional supervised machine algorithms to build our detection model in order to increase the detection rate as well as to reduce the false alarm rate. Furthermore, we prepare a much large dataset to conduct our experiments in order to comprehensively validate our proposed model.

III. PROPOSED MODEL FOR DETECTING DEFACEMENT ATTACKS

A. The Proposed Detection Model

The proposed detection model for defacement attacks is composed of two stages: the training stage and the detection stage. The training stage as shown in Fig. 5 consists of the following three steps:

- Collection of training dataset: The dataset for training is a combination of normal web-pages and defaced web-pages. Normal web-pages are downloaded from various websites in normal working conditions. Defaced web-pages are downloaded from Zone-H.org [17].
- Pre-processing: In this step, we use n-gram technique to extract the training features for each web-page's full content, including HTML code and pure text. Based on the analysis of the previous researches [11][12][13], we select 2-gram and 3-gram to extract the page features and then use the TF-IDF (Term Frequency – Inverse Document Frequency) [16] to compute the value for each feature. The result of this process is that a web-page is converted to a vector and the training dataset is transferred to the training array.
- Training: The CNN is used as the training algorithm to construct the Classifier or Model using the the training array.

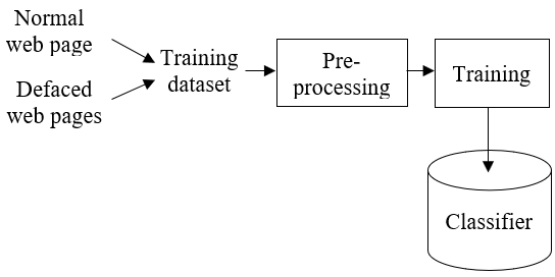


Fig. 5. Proposed detection model for defacement attacks: Training stage

The detection stage, as illustrated in Fig. 6 also includes three steps as follows:

- Collection of the monitored web-page: The HTML code of the monitored page is downloaded for pre-processing.
- Pre-processing: The monitored web-page's content is processed to extract features to form the page vector using the same method as done for each page of the training dataset.
- Classification: The page vector is classified using the Classifier built in the training stage. The result of this step is the page status of either *Normal* or *Defaced*.

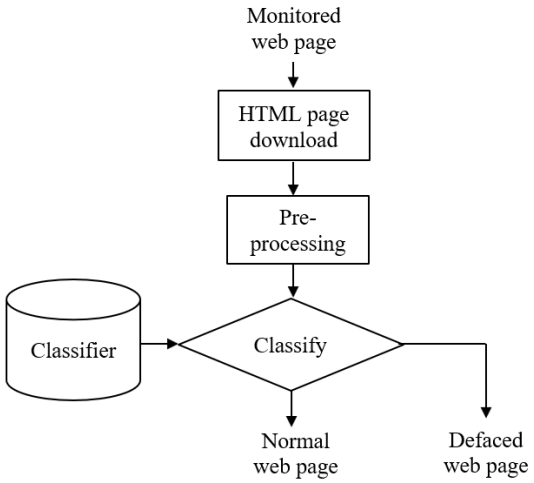


Fig. 6. Proposed detection model for defacement attacks: Detection stage

B. Training the Detection Model Using CNN

As previously mentioned, we use CNN algorithm to construct our detection model for website defacements from the training data. The CNN algorithm is selected because it is fast and it has been widely used with good performance in many computer science areas, such as image processing and recognition, natural language processing [14][15]. Fig. 7 describes the CNN structure used in the proposed model, in which a Conv_1D function, a Flatten layer and 4 fully-connected layers of Dense 1, 2, 3 and 4 to generate the output. The ELU activation function and the Softmax loss function are used in layers.

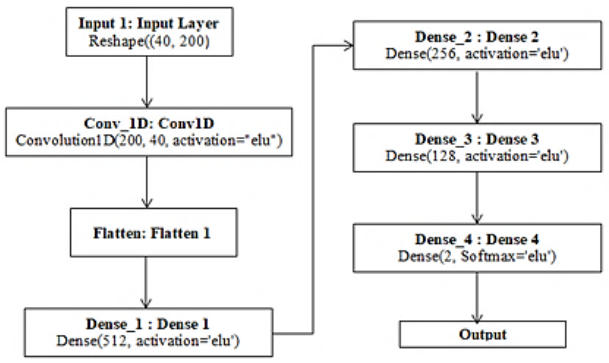


Fig. 7. The CNN structure used in the proposed detection model for website defacements

The ELU (Exponential Linear Unit) [15] function is defined as follows:

$$\mathrm{ELU} = \begin{cases} x & x > 0 \\ \alpha e^{x} - \alpha & x \le 0 \end{cases} \text{ or } \quad (1)$$

$$\mathrm{ELU}(x) = \max(0, x) + \min(0, \alpha e^{x} - \alpha))$$

where α = 1 as recommended in [15]. We select ELU function because it can produce relatively low level of error frequencies and average training time.

C. Performance Measurement

We use 6 measurements, including TPR (True Positive Rate or Recall), FPR (False Positive Rate), FNR (False Negative Rate), PPV (Positive Predictive Value or Precision), F1 (F1-Score) and ACC (Overall Accuracy) to measure the proposed model's performance as the following:

$$PPV = \frac{TP}{TP + FP} \quad (2)$$

$$TPR\ \frac{TP}{TP + FN} \quad (3)$$

$$FPR = \frac{FP}{FP + TN} \quad (4)$$

$$FNR = \frac{FN}{FN + TP} \quad (5)$$

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

$$ACC = \frac{TP + TN}{TP + FP + FN + TN} \quad (7)$$

where TP, FP, FN and TN are elements of the confusion matrix given in Table I.

TABLE I. TP, FP, FN AND TN IN THE CONFUSION MATRIX

		Actual Class	
		Defaced	*Normal*
Predicted Class	*Defaced*	TP (True Positives)	FP (False Positives)
	Normal	FN (False Negatives)	TN (True Negatives)

IV. EXPERIMENTS AND RESULTS

A. Experimental Dataset

The experimental dataset used in this paper consists of a subset of normal web-pages and another subset of defaced web-pages. We developed a small tool written in JavaScript running on the NodeJS server and the Puppeteer library to download and process HTML code of web-pages. Specifically, the two subsets of the dataset of 100,000 web-pages are as follows:

- The normal web-pages are composed of 40,000 web-pages in normal working conditions. These web-pages are home pages of well-known websites in Vietnam and in the world, including news portals, e-commerce sites, online services sites and forum sites. These websites are selected from top 1 million websites listed by Alexa [18].
- The defaced web-pages consist of 60,000 web-pages, which are collected from Zone-H.org [17]. Downloaded defaced web-pages are checked and any duplicated pages are removed.

B. Pre-processing, Training and Validation Testing

The dataset collected is pre-processed using n-grams and TF-IDF techniques to convert web-pages to the training array of web-page vectors. Based on previous works [11][12][13], we select a set of 8000 n-gram features to create web-page vectors. The vectors from normal web-pages are labelled "normal" and those from defaced web-pages are labelled "defaced". The training array is then ready for training stage to construct and validate the detection model.

We use 2 traditional machine learning algorithms of decision tree and random forest proposed by [11][12][13] for defacement detection, and the CNN algorithm in the training stage to build different defacement detection models for performance comparison. For the models based on decision tree and 50-tree random forest, 10-fold cross-validation method is used. For the CNN-based model, parameters of epochs = 64 and batch_size = 32 are used in the training and validation. For each run, 75% of the dataset are used for training and 25% of the dataset are used for validation testing. The final performance measurements are computed as the average of measured values of all runs.

C. Experimental Results and Comments

Table II provides the detection performance of our CNN-based model and the decision tree-based model [11] and the random forest (RF)-based model [12][13]. From the experimental results given in Table II, we can draw the following comments:

- Our CNN-based model performs better than previous models based on traditional supervised machine learning methods of decision tree [11] and random forest [12][13]. Specifically, our model's measurements are considerably higher than those of decision tree-based model [11]. However, the proposed model's ACC and F1 are only slightly better than those of random forest-based model [12][13].
- Although the proposed model's ACC and F1 are only slightly better than those of random forest-based model [12][13], its false alarm rates (FPR and FNR) are significantly lower than those of decision tree-based model [11] and random forest-based model [12][13]. Low false alarm rates are very important for any practical solution.

TABLE II. THE PROPOSED MODEL'S DETECTION PERFORMANCE VERSUS PERFORMANCE OF [11][12][13]

Detection models	PPV	TPR	FPR	FNR	ACC	F1
Decision tree-based model [11]	97.47	97.85	3.82	2.15	97.18	97.66
RF-based model [12][13]	98.91	98.15	1.63	1.85	98.24	98.53
Our CNN-based model	98.55	98.61	0.97	1.39	98.86	98.61

V. CONCLUSION

This paper proposes a CNN-based model for detecting website defacement attacks. In our model, we exploit the CNN's superior classification capability to solve the problem of website defacement detection. Experiments conducted on the dataset of 100,000 web-pages show that the proposed CNN-based detection model outperforms previous models based on traditional supervised machine learning methods of decision tree [11] and random forest [12][13]. Especially, the false alarm rates, including false positive and negative rates are reduced significantly compared to those of previous models.

One of the shortcomings of our model is it requires higher computing resources because CNN is generally computationally intensive than traditional supervised machine learning counterparts, such as decision tree and random forest. For future work, we will carry out an extensive assessment on all execution steps of the model and find a solution to lower its computational requirements.

REFERENCES

[1] Imperva, Website Defacement Attack, https://www.imperva.com/ learn/application-security/website-defacement-attack/, last accessed 2020/11/10.

[2] Trend Micro, The Motivations and Methods of Web Defacement, https://www.trendmicro.com/en_us/research/18/a/hacktivism-web-defacement.html, last accessed 2020/11/10.

[3] Government Technology, The Coronavirus Pandemic Moved Life Online – a Surge in Website Defacing Followed, https://www.govtech.com/security/The-Coronavirus-Pandemic-Moved-Life-Online--a-Surge-in-Website-Defacing-Followed.html, last accessed 2020/11/10.

[4] Nagios Enterprises, LLC. Web Application Monitoring Software with Nagios. https://www.nagios.com/solutions/web-application-monitoring/, last accessed 2020/11/10.

[5] Site24x7. Website Defacement Monitoring. https://www.site24x7.com/monitor-webpage-defacement.html, last accessed 2020/11/10.

[6] Banff Cyber Technologies. WebOrion Defacement Monitor. https://www.weborion.io/website-defacement-monitor/, last accessed 2020/11/10.

[7] W. Kim, J. Lee, E. Park, S. Kim. 2006. *Advanced Mechanism for Reducing False Alarm Rate in Web Page Defacement Detection*. National Security Research Institute, Korea.

[8] A. Bartoli, G. Davanzo and E. Medvet. 2010. *A Framework for Large-Scale Detection of Web Site Defacements*. ACM Transactions on Internet Technology, Vol.10, No.3, Art.10.

[9] G. Davanzo, E. Medvet and A. Bartoli. 2011. *Anomaly detection techniques for a web defacement monitoring service*. Journal of Expert Systems with Applications, 38 (2011) 12521–12530, doi:10.1016/j.eswa.2011.04.038, Elsevier.

[10] K. Borgolte, C. Kruegel and G. Vigna. 2015. Meerkat: Detecting Website Defacements through Image-based Object Recognition. In: *Proceedings of the 24th USENIX Security Symposium* (USENIX Security).

[11] X.D. Hoang. 2018. A Website Defacement Detection Method Based on Machine Learning Techniques. In SoICT '18: Ninth International Symposium on Information and Communication Technology, December 6–7, 2018, Da Nang City, Viet Nam. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3287921.3287975.

[12] X.D. Hoang, N.T. Nguyen. 2019. Detecting Website Defacements Based on Machine Learning Techniques and

Attack Signatures, Computers 2019, 8, 35; doi:10.3390/computers8020035.
[13] X.D. Hoang, N.T. Nguyen. 2019. A Multi-layer Model for Website Defacement Detection. In In SoICT'19: Tenth International Symposium on Information and Communication Technology, December 4 – 6, 2019 | Hanoi - Ha Long Bay, Vietnam. ACM, New York, NY, USA, 6 pages. *https://doi.org/10.1145/3368926.3369730*.
[14] D-A. Clevert, T. Unterthiner and S. Hochreiter. 2015. Fast and accurate deep network learning by exponential linear units (elus). Available online: https://arxiv.org/abs/1511.07289.
[15] N.K. Sangani, H. Zarger. 2017. "Machine Learning in Application Security," *Book chapter in "Advances in Security in Computing and Communications"*, IntechOpen.
[16] X.D. Hoang. 2021. Detecting Common Web Attacks Based on Machine Learning Using Web Log. In: Sattler KU., Nguyen D.C., Vu N.P., Long B.T., Puta H. (eds) Advances in Engineering Research and Application. ICERA 2020. Lecture Notes in Networks and Systems, vol 178. Springer, Cham. https://doi.org/10.1007/978-3-030-64719-3_35
[17] Zone-H.org, http://zone-h.org/?hz=1, last accessed 2020/11/10.
[18] DN Pedia – Top Alexa one million domains. Available online: https://dnpedia.com/tlds/topm.php, last accessed 2020/11/10.

MỘT MÔ HÌNH PHÁT HIỆN THAY ĐỔI GIAO DIỆN WEBSITE DỰA TRÊN CNN

Tóm tắt: Trong thập kỷ vừa qua, các cuộc tấn công thay đổi giao diện website được xem là mối đe doạ nghiêm trọng đến các website và các ứng dụng web của cơ quan, tổ chức tư nhân cũng như nhà nước. Một cuộc tấn công thay đổi giao diện có thể ảnh hưởng lớn đến chủ sở hữu của website, như tức thì làm ngừng hoạt động website, ảnh hưởng xấu đến danh tiếng của chủ sở hữu, và những điều này có thể dẫn đến những thiệt hại lớn về tài chính. Nhiều giải pháp đã được nghiên cứu và triển khai cho giám sát và phát hiện tấn công thay đổi giao diện, như các giải pháp dựa trên so sánh đơn giản và các giải pháp dựa trên các giải thuật phức tạp. Tuy vậy, một số giải pháp chỉ có thể hoạt động tốt với các trang web tĩnh và một số giải pháp khác có thể hoạt động với các trang web động, nhưng lại sinh nhiều cảnh báo sai. Bài báo này đề xuất sử dụng mạng nơ ron tích chập (CNN) để xây dựng mô hình phát hiện thay đổi giao diện. Mô hình phát hiện đề xuất là một mở rộng của các mô hình dựa trên các kỹ thuật học máy truyền thống, nhằm nâng cao tỷ lệ phát hiện đúng và giảm tỷ lệ cảnh báo sai. Các thử nghiệm thực hiện trên tập dữ liệu gồm 100.000 trang web cho thấy mô hình đề xuất cho hiệu năng phát hiện tốt hơn đáng kể so với các mô hình phát hiện dựa trên học máy truyền thống.

Từ khóa: Mô hình phát hiện thay đổi giao diện, Tấn công thay đổi giao diện website, Phát hiện thay đổi giao diện website.

Hoang Xuan Dau received the bachelor degree of informatics in 1994 at the Hanoi University of Science and Technology. He then received the master degree and PhD degree in computer science at the RMIT university, Australia in 2000 and 2006, respectively. He is currently a senior lecturer of the faculty of information technology, Posts and Telecommunications Institute of Technology. His research interests include attack and intrusion detection, malware detection, system and software security, web security, machine learning-based applications for information security.

Nguyen Trong Hung received the bachelor degree of information technology in 2013 at the Academy of People's Security. He then received the master degree in information security at the Academy of Cryptographic Techniques in 2018. He is currently a lecturer of the faculty of information technology and security, Academy of People's Security. His research interests include attack and intrusion detection, malware detection, and web security.

MAXIMUM POWER POINT TRACKING CONTROL SCHEME FOR MICRO-WIND TURBINE SYSTEM

Ho Nhut Minh[*], Nguyen Trong Huan[*], Van Tan Luong[+]
[*] Học Viện Công Nghệ Bưu Chính Viễn Thông Cơ Sở Thành Phố Hồ Chí Minh
[+] Trường Đại học Công nghiệp Thực phẩm Thành Phố Hồ Chí Minh

Abstract **-** In this paper, a maximum power point tracking (MPPT) scheme is proposed for permanent magnet synchronous generator (PMSG) wind turbine systems. With this method, an adaptive compensation control is considered to improve the system dynamic response and therefore more energy yield can be extracted from the wind turbine, depending on a trade-off between the system dynamic behavior and the transient load of the drive train. The effectiveness of the proposed methods is verified by simulation results for the 3.2[kW]-PMSG wind turbine system.

Keywords **-** Maximum power point tracking, permanent magnet synchronous generator, torque control, wind turbine.

I. INTRODUCTION

These days, variable-speed wind turbine systems have been widely used in field applications. The operation range of variable-speed system is wide and provides 10%-15% higher energy capture from the wind turbine, when compared to the fixed-speed wind turbine systems [1]. Also, the initial installation cost for variable-speed system increases since the power converter is required. However, this cost can be compensated due to the enhanced capability of the energy capture.

Several different methods such as power signal feedback control, perturbation and observation (P&O) control, tip-speed ratio control, and optimal power control have been suggested to regulate the maximum output power of the wind turbine system in the low speed region. For the power signal feedback control, the MPPT method is not difficult to implement without wind speed measurement. Also, the method is stable since the data in the look-up table is obtained by the real test [2], [3]. However, it is not easy to get the field data. Also, a P&O control method has been applied for maximum power point tracking (MPPT) [4], [5]. This algorithm has been widely used in searching for maximum power values due to its simplicity. Furthermore, the use of the P&O does not require wind speed information and turbine parameters, and it is faster and more efficient in searching the maximum point of power. However, its disadvantage is that oscillations are produced under steady-state conditions because of constant duty cycle changes [4]. As for the tip-speed ratio control, the rotational speed is regulated to keep the tip-speed ratio to be optimal [6]. This method is simple. However, the performance of the tip-speed ratio control depends on the accuracy of the wind speed measurement. On other way, the optimal power control can regulate the generator power to its optimal value which corresponds to the optimal tip-speed ratio and rotor speed [7]. With this method, the power reference is

proportional to the cubic of the rotor speed. Although this method is simple and effective, the study on the system dynamics, which is done in frequency domain, proves that its MPPT speed is low. Also, when the turbine operates at the low wind velocity, the MPPT bandwidth is narrow. Thus, energy produced is reduced and this affects electrical users. [1]

In this paper, a MPPT control method is proposed for PMSG wind turbine system. With this method, an adaptive compensation control has been applied, from which the bandwidth of the MPPT is significantly increased. Thus, transient performance of the MPPT control is also improved. Simulation results for a 3.2[kW] PMSG wind turbine system are provided to verify the validity of the proposed control strategy.

II. SYSTEM MODELING OF WIND TURBINE SYSTEMS

The configuration of the PMSG wind turbine system is shown in Figure 1, in which the machine-side converter controls the MPPT and grid-side converter regulates the DC-link voltage.

Contact: Ho Nhut Minh,
Email: minhho@ptithcm.edu.vn
Received: 15/10/2020, Revised: 10/12/2020, Accepted: 28/01/2021.

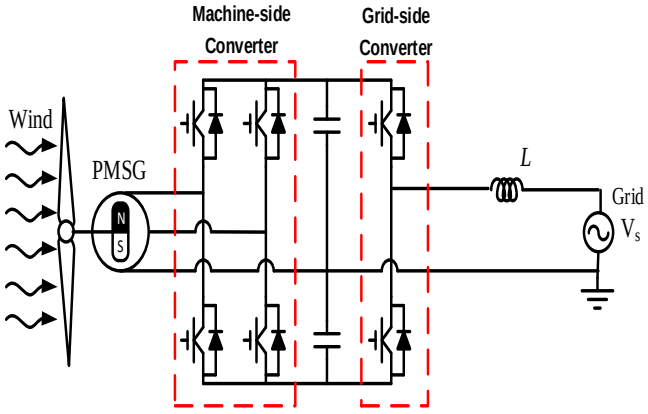


Figure 1. *Circuit configuration of small wind turbine system with PMSG.*

The turbine power of the wind turbine (P_t) is determined as [8]

$$P_t = \frac{1}{2}\rho\pi R^2 C_p(\lambda) V_w^3 \quad (1)$$

Where ρ is the air density [kg/m^3], R is the radius of blade [m], V_w is the wind speed [m/s], and $C_p(\lambda)$ is the power conversion coefficient which is a function of the tip-speed ratio, in which the tip-speed ratio is defined as [8]

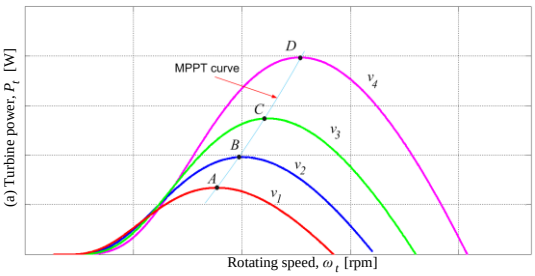
$$\lambda = \frac{\omega_t R}{V_w} \quad (2)$$

The $C_p(\lambda)$ is expressed as

$$C_P(\lambda) = \frac{1}{2}\left(\frac{116}{\lambda - 0.035} - 4.8\right)e^{\left(\frac{-21}{\lambda - 0.035}\right)} \quad (3)$$

The turbine torque is expressed as

$$T_t = \frac{0.5\rho\pi R^5 C_p(\lambda)}{\lambda^3}\omega_t^2 \quad (4)$$



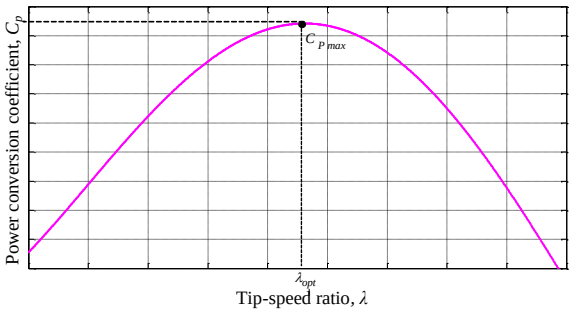


Figure 2. *Wind turbine characteristics. (a)* $P_t - \omega_t$ *curve. (b)* $C_p - \lambda$ *curve.*

As illustrated in Figure 2, the wind turbine is characterized by the ($P_t - \omega_t$) and ($C_p - \lambda$) curves. The power conversion coefficient reaches its maximum value ($C_{p\max}$) at the optimal tip-speed ratio (λ_{opt}), as shown in Figure 2(b). Also, the wind power conversion system has to operate at the λ_{opt} to maximize the C_p.

The relation between the torque and the rotor speed is expressed as [9], [10]

$$T_t - T_g = T_J = J_t\frac{d\omega_t}{dt} + \left(B_t + B_r\right)\omega_t \quad (5)$$

Where T_J is inertial torque of the rotor, J_t is the combined inertia of the turbine and generator, B_t is the damping coefficient of turbine, B_r is the intrinsic speed feedback of the turbine and T_g is the generator torque.

III. PROPOSED MPPT CONTROL

Figure 3 shows the MPPT control block diagram for the conventional control method and the proposed control method, respectively. First, the turbine speed is estimated. Then, the torque reference divided by the torque constant (k_t) commands the rotor q-axis current reference (I_{qse}^*). This MPPT control block diagram can be seen in the corresponding part in Figure 3.

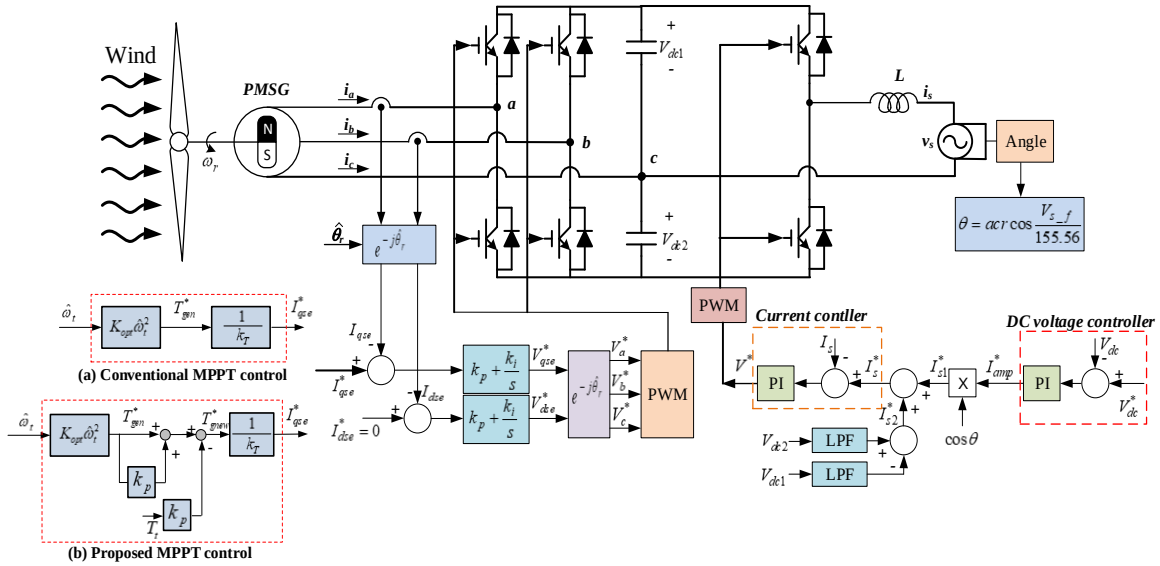


Figure 3. MPPT control block diagram. (a). Conventional MPPT control. (b). Proposed MPPT control

III.1. TURBINE SPEED ESTIMATION

A sensorless control method is applied, depending on rotor flux observer and induced electro-motive force. As can be seen from Figure 4, the stator flux (λ_s^s) is obtained from the stator voltage (v_s) and current (i_s). Then, the cut-off frequency (ω_0) of a high-pass filter is properly chosen to be one-third of the generator rated speed. Also, to remove a delay problem caused by the filter, the magnitude component, $\sqrt{\hat{\omega}_p^2+\omega_0^2}/\hat{\omega}_p$, and phase component, $e^{(\phi-\pi/2)}$, are multiplied with the function of λ_s/v_s, for compensation, in which $\phi=\arctan(\hat{\omega}_p/\omega_0)$ is the phase angle. Next, the flux linkage λ_f, is calculated from the d, q-axis rotor flux, λ_{df}^s and λ_{qf}^s, from which the rotor position angle is obtained as [11]

$$\hat{\theta}_r=\arctan\left(\lambda_{qf}^s/\lambda_{df}^s\right) \tag{6}$$

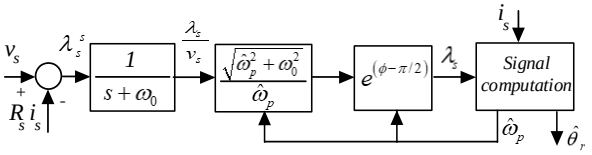


Figure 4. Block diagram of generator speed estimation.

By integrating the term of $\cos(\hat{\omega}_p t)$ in [t_0, t_1] and calculating the approximate area for the integration, $\int_{t_0}^{t_1}\cos(\hat{\omega}_p t)dt$, the estimated speed is obtained as

$$\hat{\omega}_p=\frac{\sin\hat{\theta}_{r1}-\sin\hat{\theta}_{r0}}{(\cos\hat{\theta}_{r1}+\cos\hat{\theta}_{r0})T_s/2} \tag{7}$$

where $\hat{\theta}_{r1}=\hat{\omega}_p t_1$, $\hat{\theta}_{r0}=\hat{\omega}_p t_0$, and T_s is a sampling time.

A low-pass filter is applied to reduce the speed ripple at the high frequencies to get the average generator speed, $\hat{\omega}_r$. The estimated turbine speed, $\hat{\omega}_t$, is obtained from $\hat{\omega}_r$.

III.2. MPPT METHOD

For a conventional MPPT controller, when the C_p reaches $C_{p\max}$ and the λ reaches λ_{opt}, the torque reference is obtained from (4) as follows

$$T_{gen}^*=K_{opt}\hat{\omega}_t^2 \tag{8}$$

where $K_{opt}=0.5\rho\pi R^5 C_{p\max}(1/\lambda_{opt})^3$.

To increase the annual energy yield, an improved MPPT control strategy is applied, in which the adaptive compensation gain (k_p) is added to the controller to determine the transient performance of the MPPT control. Thus, the new torque reference (T_{gnew}^*) is obtained as

$$T_{gnew}^*=K_{opt}\hat{\omega}_t^2\left(1+k_p\right)-k_p T_t \tag{9}$$

It can be seen from (9) that k_p is used as an adaptive compensation, to improve faster performance of the turbine speed. Thus, more extracted energy can be captured.

Hence, the relation between the torque and the rotor speed for the proposed MPPT method is expressed as

$$T_t-T_{gnew}^*=J_t'\frac{d\hat{\omega}_t}{dt}+\left(B_t'+B_r'\right)\hat{\omega}_t \tag{10}$$

where $J_t'=J_t/(1+k_p)$ and $B_t'+B_r'=\left(B_t+B_r\right)/(1+k_p)\cdot$

As illustrated in Figure 5, the proposed MPPT controller is considered when there is the step change of wind velocity from V_{w1} to V_{w2}. Due to the inertia of the wind power generation system, the generator speed cannot follow the sudden speed change immediately. For a conventional MPPT controller, the torque reference T_{gen}^* is obtained from (8) during the transient state. However, as the wind velocity is changed to V_{w2}, the optimal torque is located at

point *B*. The solid trajectory between A and B is not really optimal one. The dynamic response for turbine acceleration at point *B* will be relatively slow (see dash line). On the other hand, by using the proposed MPPT controller, due to the adaptive compensation, the new torque reference will be smaller than that of the conventional optimal torque (conventional MPPT) controller to increase the torque difference for accelerating faster to point *B*. Thus, during the period of the wind speed variation, the amount of the extracted wind energy is significantly increased by using the proposed MPPT controller.

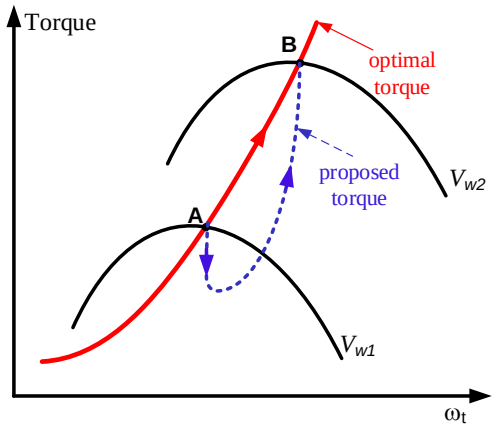


Figure 5. Turbine torque versus rotor speed

III.3. OPTIMIZED CONTROL OF SYSTEM DYNAMICS

As aforementioned, the proposed MPPT control method can make the maximum power point tracking speed much faster than that of the optimal one. The acceleration effect of the wind turbine is mainly generated by the gain (k_p). Thus, the k_p should be optimized through optimizing the bandwidth of the control system.

Using small signal analysis to (5) at the operating point *M* (V_{wM}, ω_{tM}), the system dynamics can be achieved as a first-order system:

$$(T_s s+1)\Delta\omega_t = 0 \qquad (11)$$

where

$$\begin{cases} T_s = \dfrac{J_t}{B_t + B_r + 2K_{opt}\cdot\omega_{tM} - K_{rr}} \\ K_{rr} = \dfrac{\partial T_t}{\partial \omega_{tM}} = \dfrac{1}{2}\rho\pi R^3 V_w^2 \left(\dfrac{\partial C_p(\lambda)}{\partial\lambda}\dfrac{\partial\lambda}{\partial\omega_{tM}}\right) \end{cases} \qquad (11)$$

$\partial C_p(\lambda,\beta)/\partial\lambda$ and $\partial C_p(\lambda,\beta)/\partial\beta$ in (11) are approximately zero when the system operates around the maximum power point and below the rated wind speed, respectively. Thus, the cut-off frequency of the control system dynamics can be obtained as

$$\omega_c = \frac{2K_{opt}}{J_t}(1+k_p)\omega_{tM} \qquad (12)$$

From (12), adaptive compensation gain k_p which can give faster MPPT speed, is achieved as

$$1+k_p = \left(\frac{J_t}{2K_{opt}}\right)\frac{\omega_c}{\omega_{tM}} \qquad (13)$$

According to van der Hoven spectrum, the ω_c can be selected between 0.01 [cycles/h] and 1000 [cycles/h], corresponding to the bandwidth range from $2.7\cdot10^{-6}$ [Hz] to 0.28 [Hz] [12]-[14]. The ω_c should be set to be wide enough to extract more energy from the wind turbine. In this research, ω_c is suggested to be 0.264 [Hz] (950 [cycles/h]).

IV. SIMULATION RESULTS

To verify the effectiveness of the proposed method, the simulation has been carried out using the PSIM software for a 3.2[kW]-PMSG wind turbine. The parameters of the wind turbine and generator are listed in Table 1 and 2, respectively.

Table 1. Parameters of wind turbine

Rated power	3.2[kW]
Blade radius	1.22838 [m]
Air density	1.225[kg/m^3]
Max. power conv. coefficient	0.35
Optimal tip-speed ratio	10.6
Cut-in speed	3[m/s]
Cut-out speed	25[m/s]
Rated wind speed	15.8 [m/s]
Blade inertia	0.021 [kg.m^2]

Table 2. Parameters of generator

Rated power	3.2 [kW]
Rated flux	0.468 Wb
Moment of inertia	0.021 [kg.m^2]
Stator resistance	0.49 [Ω]
Stator inductance	5.35[mH]
Number of poles	6

Figure 6 and 7 shows the dynamic responses of the conventional MPPT method and the proposed method, respectively when the wind speed changes from 10 m/s to 14 m/s at 6 sec and back to 10 m/s at 7 sec. The power conversion coefficient (C_P) which is shown in Figure 4(b), is recovered to C_{Pmax} in 0.3 sec after there is a sudden drop at 7 sec during the wind speed changes. Meanwhile, it takes about 0.2 sec for the proposed method (Figure 7(b)). Compared with the conventional MPPT method, the C_P variation gives the faster response during the step-wise wind speed change. As can be illustrated in Figure 6(c), the generator torque also varied, and then, reaches a steady state after 0.5 sec. However, for the proposed method as shown in Figure 7 (c), this value shows faster performance than that of the conventional MPPT one. Also, the actual turbine power and the maximum turbine power are shown Figure 6(d) and 6(d), respectively. For both the conventional and the proposed MPPT methods, the actual

turbine power is 1000 W at the wind speed of 10 m/s and reaches abot 2800 W at at the wind speed of 14 m/s. However, the actual turbine power in the proposed MPPT method reaches a steady state after just 0.15 sec, compared with the conventional MPPT one. As can be seen from Figures 6 (d) and 7 (d), the proposed MPPT control method gives good performance. It is evaluated with the proposed MPPT method, the energy production is 0.4 % larger than that of with the conventional MPPT control method. As the rotor speed changes as quickly as the wind speed, more turbine power can be generated. The turbine speed is well estimated, as shown in Figure 6(e) and 7(e) without using speed sensor.

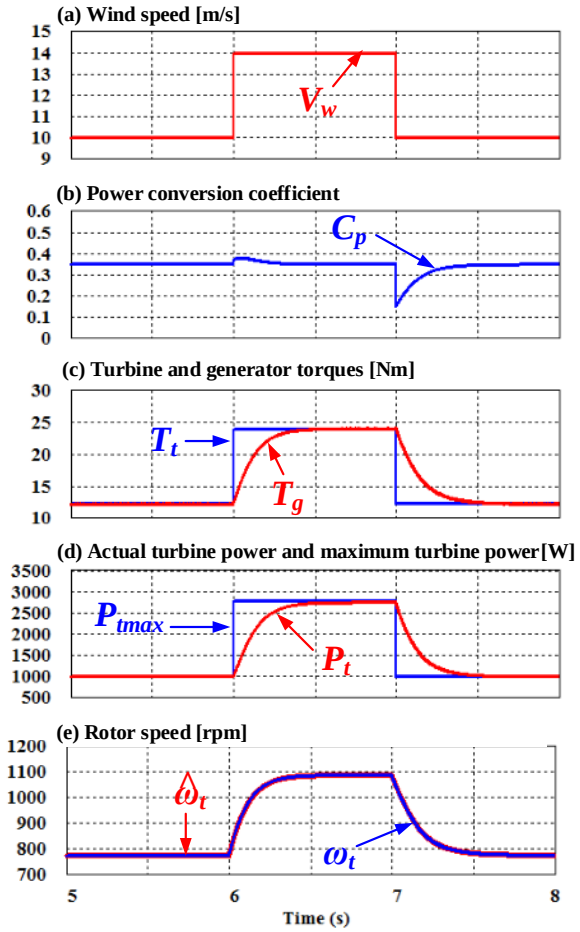


Figure 6. *Performance responses of conventional MPPT method in stepwise wind speed (a) Wind speed (b) Power conversion coefficient (c) Turbine and generator torques (d) Actual turbine power and maximum turbine power (e) Rotor speed.*

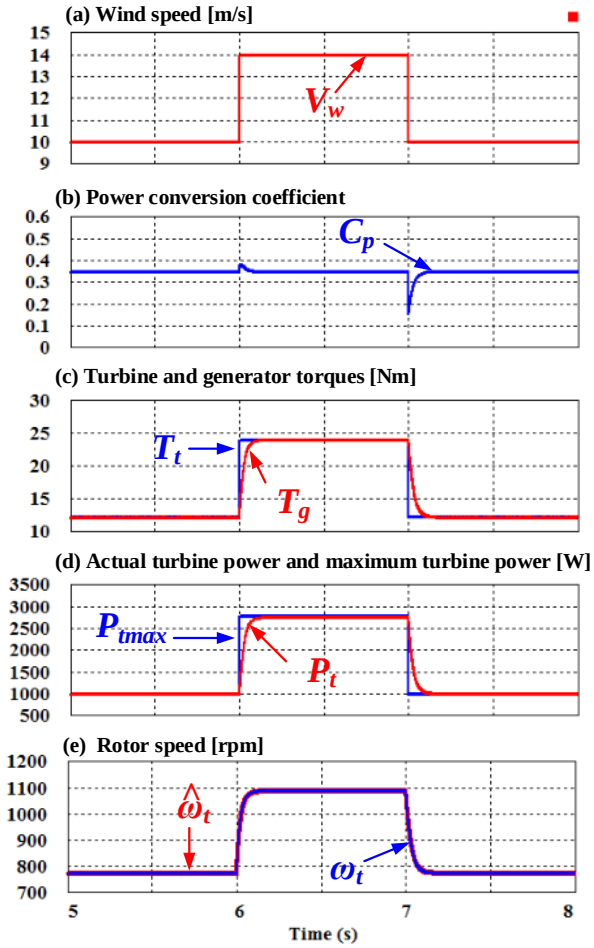


Figure 7. *Performance responses of proposed method in stepwise wind speed (a) Wind speed (b) Power conversion coefficient (c) Turbine and generator torques (d) Actual turbine power and maximum turbine power (e) Rotor speed.*

V. CONCLUSION

This paper has proposed an improved MPPT method for PMSG wind turbine systems considering the inertia torque. Through adding the adaptive compensation gain to torque, the bandwidth of the MPPT is greatly increased, from which the rotational speed is increased to improve the faster dynamic performance. For this, the amount of energy produced from wind turbine system can be annually increased (the energy production in the MPPT proposed method is 0.4 % larger than that of with the conventional MPPT control method). The validity of the control algorithm has been verified by simulation results for a 3.2[kW] PMSG wind power system.

REFERENCES

[1] Wang Q. and Chang L. (2004), An intelligent maximum power extraction algorithm for inverter-based variable speed wind turbine systems, *IEEE Transactions on Power Electronics*, vol. 19, No. 5, pp. 1242-1249.

[2] Ermis M., Ertan H. B., Akpinar E., and Ulgut F. (1992), "Autonomous wind

energy conversion systems with a simple controller for maximum-power
transfer", Proceedings on Inst. Electric. Eng. B, vol. 139, pp. 421-428.

[3] Barakati S. M., Kazerani M., Aplevich J. D. (2009), Maximum power tracking control for a wind turbine system including a matrix converter, *IEEE Transactions on Energy Conversion*, vol. 24, pp.705-713.

[4] Farhat S., Alaoui R., Kahaji A., Bouhouch L., Ihlal A. (2015), "P&O and Incremental Conductance MPPT Implementation", *International Review of Electrical Engineering*, Vol. 10, No. 1, pp. 116–122.

[5] Ramadoni S., Indah S. (2019), "Performance Improvement for Small-Scale Wind Turbine System Based on Maximum Power Point Tracking Control", *Energies*, Vol. 12, No. 3938, pp. 1-18.

[6] Hua G. and Geng Y. (2006), A novel control strategy of MPPT tracking dynamics of wind turbine into account, *in Proceedings of IEEE Power Electronics Specialist Conference*, pp. 1-6.

[7] Cardenas R. and Pena R. (2004), Sensorless vector control of induction machines for variable-speed wind energy applications, *IEEE Transactions on Energy Conversion*, vol. 19, No. 1, pp.196-205.

[8] Morimoto. S, Nakayama. H, Sanada. M and Takeda. Y (2005), Sensorless output maximization control for variable-speed wind generation system using IPMSG, *IEEE Transactions on Industry Application*, vol. 41, No. 1, pp. 60-27.

[9] Nguyen T. H. , Hosani K. A., Sayari N. A., (2016), "Grid integration improvement for single-phase inverters of small wind turbines under distorted voltage conditions", *International Journal of Electrical Power & Energy Systems*, Vol. 87, pp. 144-153.

[10] AKHMATOV, V. (2005), Induction generators for wind power, *Multi-Science Publishing Company*.

[11] Van T. L., Truong T. H., Nguyen B. P. N. T., and Trang T. T. (2013), "Nonlinear Control of PMSG Wind Turbine Systems", *Lecture notes in electrical engineering*, Vol. 282, pp.113-124.

[12] LUBOSNY, Z. (2003), Wind turbine operation in electric power system, *Springer-Verlag Berlin Heidelberg*, New York, Chap. 5.

[13] Bianchi F. D., Battista H. D. and Mantz R. J. (2007), Wind turbine control systems. *Germany: Springer*.

[14] Fernando D. Bianchi, Hernan De Battista, and Ricardo J. Mantz (2007), Wind turbine control systems, principles, modeling and gain scheduling design, *Springer*-Verlag London Limited.

[15] Leon F., David I. (2008), Renewable energy in power system, *John Wiley & Sons.*

CHIẾN LƯỢC ĐIỀU KHIỂN PHÁT CÔNG SUẤT CỰC ĐẠI CỦA HỆ THỐNG TUA BIN GIÓ CÔNG SUẤT NHỎ

Tóm tắt: Trong bài báo này, chiến lược tìm điểm phát công suất cực đại (MPPT) được đề xuất trong hệ thống tua bin gió dùng máy phát điện đồng bộ nam châm vĩnh cửu (PMSG). Với phương pháp đề xuất này, điều khiển bù thích nghi được xem xét để cải thiện đáp ứng động của hệ thống và do đó nhiều năng lượng hơn được trích ra từ tua bin gió, tùy thuộc vào sự cân bằng động giữa hệ thống và tải của bộ truyền động. Hiệu quả của các phương pháp đề xuất được xác minh bằng kết quả mô phỏng cho hệ thống tua bin gió dùng máy phát PMSG công suất 3,2 [kW].

Từ khóa - tìm điểm phát công suất cực đại, máy phát đồng bộ loại nam châm vĩnh cữu, điều khiển mô men, tua bin gió.

Ho Nhut Minh was born in Vietnam in 1987. He received his undergraduate degree in 2010, major in Electronics & Telecommunications Engineering from University of Technical Education of Ho Chi Minh City. In 2014, he received the Master of Telecommunication Engineering Degree from Posts and Telecommunications Institute of Technology, Ho Chi Minh City Campus. He is working at Department of Electrical and Electronic Engineering, Posts and Telecommunications Institute of Technology, Ho Chi Minh City Campus, VietNam.

Nguyen Trong Huan was born in VietNam in 1986. He received his undergraduate degree in 2010, major in Electrical and Electronics Technology from University of Technical Education of Ho Chi Minh City. In 2014, he received the Master of Telecommunication Engineering Degree from Posts and Telecommunications Institute of Technology, Ho Chi Minh City Campus. He is working at Department of Electrical and Electronic Engineering, Posts and Telecommunications Institute of Technology, Ho Chi Minh City Campus, VietNam.

Van Tan Luong was born in Vietnam. He received the B.Sc. and M.Sc. degrees in electrical engineering from Ho Chi Minh City University of Technology, Ho Chi Minh city, Vietnam, in 2003 and 2005, respectively, and Ph.D. degree in electrical engineering from Yeungnam University, Gyeongsan, South Korea in 2013. Currently, he is working at Department of Electrical and Electronics Engineering, Ho Chi Minh city University of Food Industry. His research interests include power converters, machine drives, wind power generation, power quality and power system