Journal of ELECTRICAL ENGINEERING, VOL 73(2022), NO4, 299–304

sciendo

PAPERS

A concept for discrimination of electrical fault from cyber attack in smart electric grid

Aniruddha Agrawal, Shaik Affijulla[1]

This letter proposes a concept to discriminate an electrical fault from a cyber attack in the modern power system. A cyber attack factor is introduced which may mislead the bus voltage stability virtually at load buses. The proposed cyber attack models are validated by executing multiple cyber attacks at a time on Western system coordinating council (WSCC) 9 bus test power system by using Siemens PSS/E and MATLAB softwares. Further, the impact of electrical fault and cyber attack on the WSCC 9 bus test power systems voltage stability has been analysed to develop a discrimination algorithm in reference to chosen load index. Despite its simplicity, the proposed discrimination algorithm is robust, accurate and quite suitable to develop intelligent measures for mal-operations against cyber attacks in the smart electric grid.

K e y w o r d s: cyber attack, electrical fault, grid operator, load index, smart grid, voltage stability

1 Introduction

In 21st century, the traditional power grid has been transformed to smart grid by integration of extensive communication technology, and sophisticated electronics with networking ability, and represents a typical cyber physical system (CPS) [1], [2]. Cyber attacks are a major threat to such CPSs, and interestingly, the impact of cyber attack depicts fault like behaviour. Thus, it is necessary to discriminate the electric fault from cyber attack for execution of the designed protection schemes in the modern power system.

In literature, various security measures for detection and mitigation of cyber attack in power system have been discussed. In [3], the technique based on k-connected communication topology is suggested to prevent denial of service (DoS) attacks. The authors of [4] have presented a summary of false data injection attack detection algorithms. In [5] the technique based on mirroring is discussed to prevent cyber attacks on PLCs based on detection of start stop attacks. Advance encryption algorithms have been developed in [6] to ensure data security. In [7], the impact of a cyber attack on the system frequency and an intrusion detection system to restore system stability has been developed. However till date, no research is addressed to discriminate electrical fault from cyber attacks in the modern power system.

In this letter, a concept has been proposed to distinguish an electrical fault and cyber attack in the complex modern power system. This may form a basis for the accurate identification of the occurrence of such disturbances in the power system; and for subsequent control actions against respective disturbances by the electric grid operator at energy management center.

We describe the proposed cyber attack models, cyber attack factor, behaviour of power system under cyber attack, and the proposed discrimination algorithm. The efficacy of proposed discrimination algorithm is discussed together with the proposed discrimination concept.

2 Problem formulation

Currently and in future, smart grids are equipped with a massive number of phasor measurement units (PMUs) which are located at every substation in the smart electric grid. Moreover, these PMUs transfer the measured system vital parameters *ie* voltage, current, frequency, *etc* to the energy management center through sophisticated communication infrastructure. Thus, a cyber attacker may easily manipulate power system state data *ie* bus voltages and line currents. Further, to execute an effective cyber attack, the attacker may manipulate data to resemble electrical fault dynamics.

Due to the peculiar nature of the power system, it is challenging to model current dynamics. However, voltage may be accurately modelled to match the electrical fault voltage dynamics. Hence, in this letter the voltage of the system has been selected as the state variable to be compromised during cyber attack. The cyber attacker may modify the voltage magnitude ($|V|$), or the voltage angle (δ), or both together.

2.1 Modelling of cyber attack

During cyber attack the voltage angle at i^{th} bus (δ_i) may be misrepresented with a specific scaling factor to δ_i^* and mathematically expressed as

$$\delta_i^* = \mathfrak{F}_1 \delta_i, \tag{1}$$

[1] Department of Electrical Engineering, National Institute of Technology Meghalaya, Shillong, Meghalaya, 793003 India, agrawalaniruddha2@gmail.com, shaik.affijulla@nitm.ac.in

https://doi.org/10.2478/jee-2022-0039, Print (till 2015) ISSN 1335-3632, On-line ISSN 1339-309X

where, $\mathfrak{F}_1$ is cyber attack factor (CAF) based on the above modelled cyber attack and can be computed through offline procedure as described in section 2.3.

Manipulated voltage at i^{th} bus can be expressed as

$$V_i^* = |V_i| \angle \delta_i^*. \tag{2}$$

Further, a cyber attacker may compromise the voltage by misleading voltage magnitude ($|V_i|$) and voltage angle (δ_i) at i^{th} bus to $|V_i|^*$ and δ_i^* with a specific scaling factor and mathematically expressed as

$$\begin{aligned} \delta_i^* &= \mathfrak{F}_2 \delta_i \\ |V_i|^* &= \mathfrak{F}_2 |V_i| \end{aligned}, \tag{3}$$

where, $\mathfrak{F}_2$ is cyber attack factor (CAF) based on the above modelled cyber attack and can be computed through off line procedure as described in section 2.3.

Manipulated voltage at i^{th} bus can be expressed as

$$V_i^* = |V_i|^* \angle \delta_i^*. \tag{4}$$

2.2 Voltage stability index under cyber attack

The power system is said to remain in stable state when it retains voltage stability. Load index L has been chosen in this work as the voltage stability index, due to its low computational burden which enables the grid operator to carry out online simulations during detection of anomalies. The L index close to 0 implies high voltage stability whereas close L index and described as

$$L_j = \left| 1 - \sum_{p=1}^{g} F_{jp} \frac{V_p}{V_j} \right|, \tag{5}$$

where, $p \in \{1 \text{ to } g\}, j \in \{g+1 \text{ to } n\}$, g is the number of generator buses, n is the size of power system, V_p, V_j represent corresponding voltage at the generator and load buses for a given configuration of power system.

The misled index (L_j^*) at j^{th} bus due to cyber attack at i^{th} bus which leads to inaccurate visualization of voltage stability by the electriv grid operator can be expressed as

$$L_j^* = \begin{cases} \left| 1 - \sum_{p=1}^{i-1} F_{jp} \frac{V_p}{V_j} - F_{ji} \frac{V_i^*}{V_j} - \sum_{p=i+1}^{g} F_{jp} \frac{V_p}{V_j} \right|, \\ \quad \text{if} \quad i \in p \\ \left| 1 - \sum_{p=1}^{g} F_{jp} \frac{V_p}{V_j^*} \right|, \quad \text{if} \quad i = j \end{cases}, \tag{6}$$

where, V_i^* and V_j^* are as per(2) and (4) respectively.

2.3 Computation of cyber attack factor

A cyber attack factor (CAF) is proposed for utilization during cyber attack to misrepresent the state data as discussed in section 2.1. The off-line procedure to compute CAF is described as follows

Algorithm: Computation of CAF
Result: CAF
Input: $|V|, \delta$ at each bus
Initialize: $\mathfrak{F} \leftarrow 0, a \leftarrow True$
while a **do**
  $\mathfrak{F} \leftarrow \mathfrak{F} + \Delta\mathfrak{F}$
  for $j \leftarrow (g+1)$ **to** n **do**
    $L_j \leftarrow L_j^*$
    if $L_j \geq (L_{\max} - \beta)$ & $L_j < 1$ **then**
      $a \leftarrow False$
      break
    end
  end
end
$\mathfrak{F} \leftarrow$ CAF
Repeat for different loading conditions

In this algorithm, $\Delta\mathfrak{F}$ denotes the step size which governs the accuracy of CAF and its value of 0.001 is considered in this paper; β is a tolerance factor depending on the attacker and its value is considered as 0.02 for WSCC 9 bus system.

During a cyber attack, the attacker experiments with various possibilities to manipulate the state data to ensure critical stability in the system. The limits for attacker

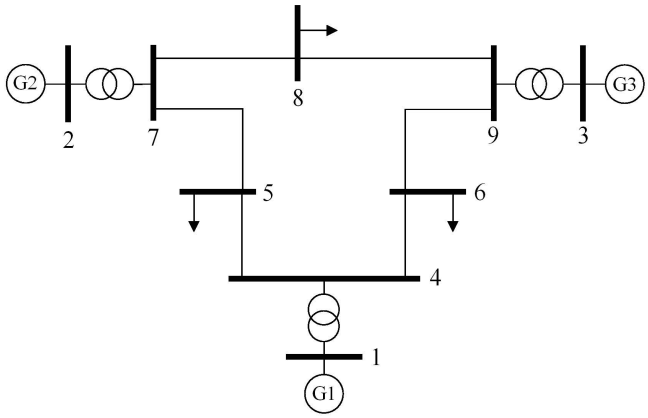

Fig. 1. Single line diagram of WSCC 9 bus test power system

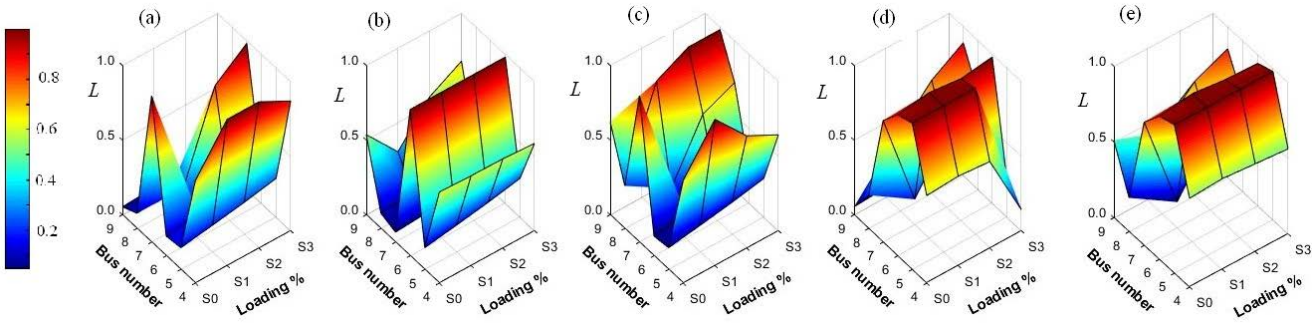

Fig. 2. Multiple buses simultaneously under cyber attack due to change in δ : (a) to (e) denote attack size of {2 to 6} on WSCC 9 bus WSCC 9 bus test system

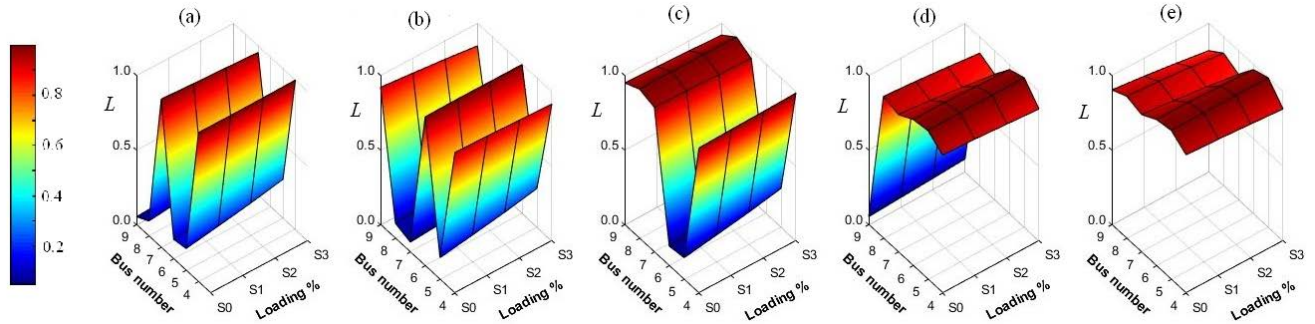

Fig. 3. Multiple buses simultaneously under cyber attack due to change in δ and $|V|$: (a) to (e) denote attack size of {2 to 6} on WSCC 9 bus test system

to mislead data are defined by $[\min, \max] \in \{\lambda\mathfrak{F}, \mathfrak{F}\}$, where, λ is the cyber attacker factor. The value of λ is unique and constant which is empirically considered in the range between 0.8 to 0.85 depending upon the configuration of modern power system.

2.4 Behaviour of power system under cyber attack

To reveal the behaviour of power system under proposed cyber attacks *ie* (2) and (4), the WSCC 9 bus test system is considered as shown in Fig. 1. In [9] and [10], authors have analysed the impact of proposed cyber attack at a bus and explored the nature of cyber attacks on power system respectively. Further, the authors have analysed the impact of proposed cyber attacks on WSCC 9 bus test power system through rigorous simulations on multiple buses at a time.

The WSCC 9 is exposed to multiple cyber attacks *ie* due to change in δ *ie* (2) and due to change in δ and $|V|$ *ie* (4) simultaneously on selected buses with a capacity of attack size ranging from 2 to 6. The L index at load buses *ie* 4 to 9 is computed during above cyber attacks under various loading cases of the power system from base load (S0) to 60% above base load (S3) varied in steps of 20%, through the voltage stability analysis of the power system under the proposed cyber attack models *ie* (2) and (4) as depicted in Fig. 2 and Fig. 3. It is revealed that the impact of cyber attack resembles fault like behaviour.

It is observed that based on the bus under attack, the power system is virtually transformed to unstable. For instance, from Fig. 2(E) it is observed that the buses 5, 6 have been transformed to voltage unstable *ie* $L > 0.85$. From Fig. 3(B) it is observed that the buses 4, 6, 9 have been transformed to voltage unstable *ie* $L > 0.85$. Hence, the authors have subsequently proposed an algorithm to discriminate an electrical fault from a cyber attack in the modern electric grid.

2.5 Proposed discrimination algorithm

In this letter, a rigorous proposed cyber attacks and electrical fault (single phase fault with line to ground impedance varying from 0 to 1000 Ω, and three phase fault) simulations have been performed on WSCC 9 bus test system under various loading cases from base load (S0) to 60% above base load (S3) varied in steps of 20%. The impact on voltage stability in terms of L index has been analyzed under above scenarios. Based on rigorous study, an algorithm is proposed to discriminate an electrical fault and cyber attack as shown in Fig. 4.

3 Simulation results

To validate the proposed discrimination concept, the Western System Coordinating Council (WSCC) 9 bus

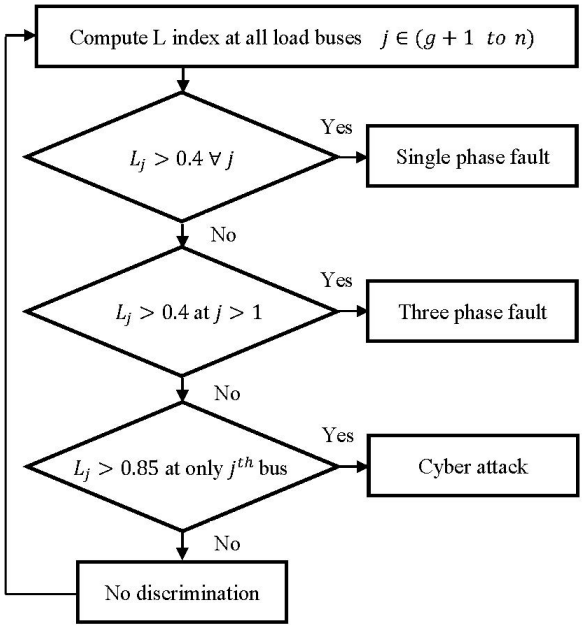

Fig. 4. Flowchart for discrimination of electrical fault and cyber attack

test system is considered as shown in Fig. 3(a). The proposed cyber attacks as discussed in section 2.1, and various electrical faults have been simulated on several buses of WSCC 9 bus test system by utilizing Siemens PSS/E and MATALB softwares. The cyber attack or electric fault is initiated at a single bus under different loading scenarios in the WSCC 9 bus test system. Further, the impact analysis is performed in reference to voltage stability as discussed in section 2.2 and the efficacy of proposed algorithm to distinguish the electrical fault and cyber attack is presented.

3.1 Cyber attack factor values

The CAF has been utilized to mislead the voltage stability in the power system. For execution of cyber attack due to change in δ and both δ and $|V|$, the required CAF scenario is shown in Fig. 5 and Fig. 6.

In Fig. 5, it should be noted that the 'zero' value at various buses $(2,\ 3,\ 7,\ 8)$ and different loading scenarios $(S2,\ S1,\ S1,\ S0)$ respectively represent the value of CAF *ie* $\mathfrak{F} > 45$. Cyber attack at slack bus has not been considered as voltage magnitude and angle can be controlled through exciter and speed governor respectively.

3.2 Validation of proposed discrimination algorithm

To showcase the efficacy of proposed discrimination concept, a cyber attack and several electric faults are simulated at a load bus *ie* bus 5 in the WSCC 9 bus test power system. The simulation results under above scenarios with varying loading conditions are shown in Fig. 7. It can be observed that only bus 5; buses 4, 5 and buses 4 to 9 depict voltage instability in terms of L index during cyber attack, LLL fault and LG fault at bus 5 respectively. Thus, in reference to proposed discrimination concept as discussed in Section 2.5, the discrimination between electrical fault and cyber attack is successfully executed on WSCC 9 bus test system.

Similarly, the above scenarios are analysed at a generator bus *ie* bus 2 to evaluate the performance of proposed discrimination algorithm and the results are shown in Fig. 8. It is revealed from simulation results that bus 7 (due to configuration of system) depicts voltage instability during cyber attack and during various electrical faults with similar behaviour in terms of L index under different loading conditions. Thus, load index may not be suitable to discriminate electrical fault from cyber attack at generator buses which is generally difficult to execute by the attacker in the electric grid.

Hence, an extensive research should be focused in the direction of proposed discrimination concept with the suitably derived power system parameters by considering voltage/current phasor, frequency, impedance, complex power, etc. Therefore, the proposed discrimination concept can be best suitable and support to develop sensitive cyber attack and electrical fault discrimination algorithms by the power system researchers for securing the smart electric grid.

Conclusions

From the proposed work, it is interesting to note that an electrical fault can be discriminated from a cyber at-

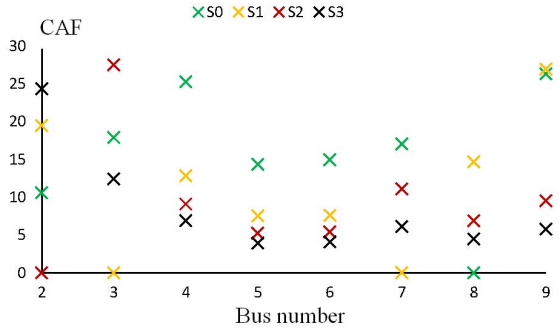

Fig. 5. CAF scenario on WSCC 9 bus system due to change in δ

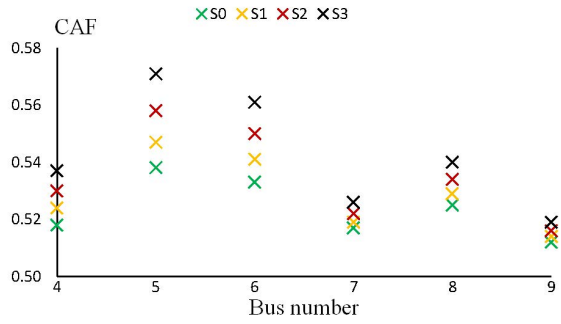

Fig. 6. CAF scenario on WSCC 9 bus system due to change in both δ and $|V|$

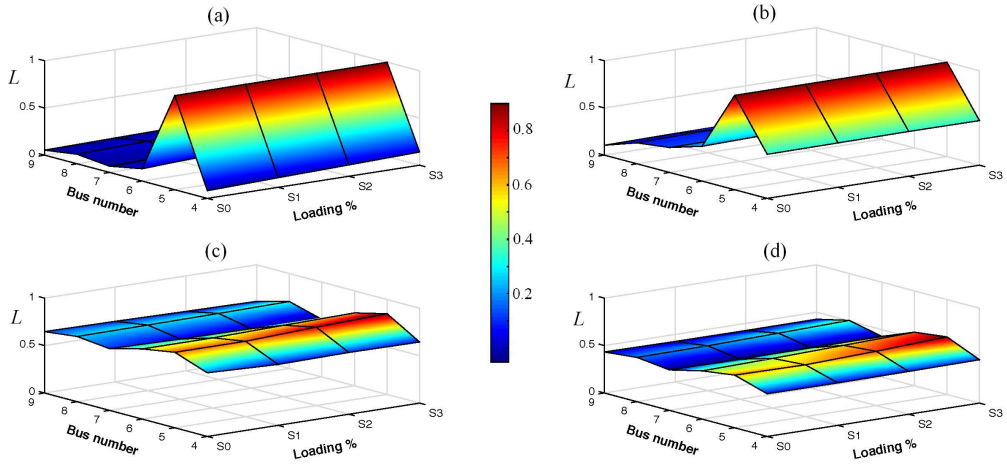

Fig. 7. Impact analysis of cyber attack and electrical fault on load bus: (a) – impact of cyber attack, (b) – impact of three phase fault, and (c), (d) – impact of single phase fault with 600 Ω and 1000 Ω

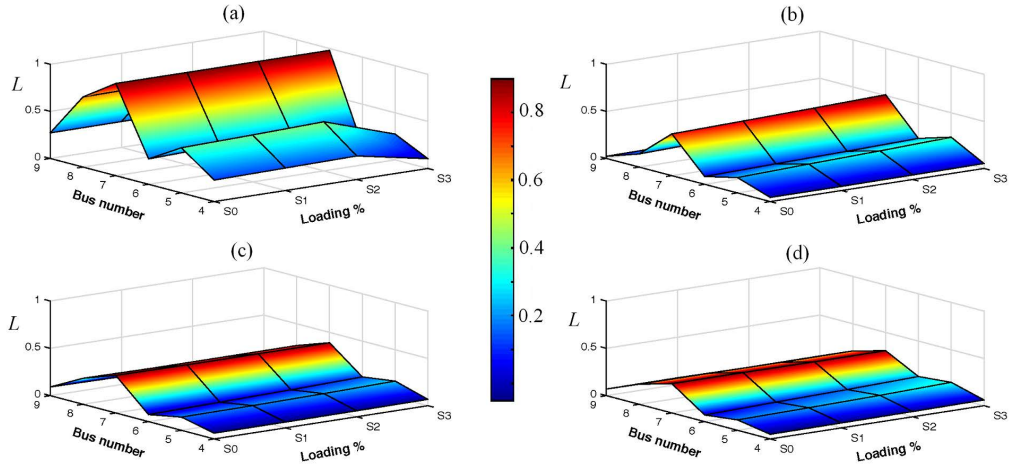

Fig. 8. Impact analysis of cyber attack and electrical fault on generator bus: (a) – impact of cyber attack, (b) – impact of three phase fault, ans (c), (d) – impact of single phase fault with 600 Ω and 1000 Ω

tack based on system voltage stability. The simulation results reveal that

- A cyber attack/electrical fault at generator bus leads the buses to voltage instability based on configuration of the power system.
- When an cyber attack is executed at load bus, only the attacked bus shows voltage instability, $L > 0.85$.
- When an electrical fault occurs on load bus, multiple load buses turn unstable depending on the nature of fault, $L > 0.4$.

Thus, the proposed work can be utilized by the grid operator/researchers to develop intelligent measures during cyber attack and prevent the smart electric grid from mal-operations.

In this letter, the discrimination algorithm has been proposed based on cyber attack and electrical fault at a single bus at a time. In the future, the authors aim to develop an algorithm to discriminate a cyber attack from an electrical fault based on multiple buses under cyber attack and electrical fault at a time in the smart electric grid.

References

[1] Z. El-Mrabet, *et al*, "Cyber-security in smart grid: Survey and challenges", *Computers and Electrical Engg*, vol. 67, pp. 469-482, 2018.

[2] V. D. Lecce, A. Amato, *et al*, "Bigraph Theory for Distributed and Autonomous Cyber-Physical System Design", *IAENG International Journal of Computer Science*, vol. 47, no. 1, pp. 37-46, 2020.

[3] T. Zhang and D. Ye, "Distributed secure control against denial-of-service attacks in cyber-physical systems based on K-connected communication topology", *IEEE Transactions on Cybernetics*, pp. 1-9, 2020.

[4] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids", *IEEE Transactions on Smart Grid*, pp. 1-17, 2019.

[5] E. N. Yılmaz and S. Gönen, "Attack detection / prevention system against cyber attack in industrial control systems", *Computers and Security*, vol. 77, pp. 94-105, 2018.

[6] E. B. Nababan, G. T. Simbolon, *et al*, "Multi-LSB and Modified Vernam Cipher to Enhance Document File Security", *IAENG International Journal of Computer Science*, vol. 47, no. 4, pp. 705-712, 2020.

[7] A. Stefanov and C. Liu, "Cyber-power system security in a smart grid environment", *IEEE PES Innovative Smart Grid Technologies (ISGT)*, Washington DC, USA, 2012, pp. 1-3.

[8] D. M. Shah, S. Tomonobu, *et al*, "A Recap of voltage stability indices in the past three decades", *Energies*, vol. 12, pp. 1-18, 2019.

[9] A. Agrawal, D. M. Momin, D. Syndor, and S. Affijulla, "Impact analysis of cyber attack under stable state of power system: voltage stability", *IEEE Region 10 Symposium*, Dhaka, Bangladesh, 2020, pp. 402-405.

[10] A. Agrawal, D. Syndor, D. M. Momin, and S. Affijulla, "Theorems to explore the nature of cyber attacks on power system voltage stability", *De Gruyter International Journal of Emerging Electric Power Systems*, pp. 1-14, 2021. doi.org/10.1515/ijeeps-2021-0176.

Received 25 July 2022

Aniruddha Agrawal received the BTech degree in Electrical and Electronics Engineering from National Institute of Technology Meghalaya, Shillong, India in 2020. Currently, he is pursuing the Master degree at McMaster University, Hamilton, Ontario, Canada. His current research interests include smart grids, electrical machine design, electric motor drives and power converter systems.

Shaik Affijulla received the MTech degree in Electrical Engineering from National Institute of Technology Hamirpur, Himachal Pradesh, India in 2011 and PhD degree in Electrical Engineering from National Institute of Technology Meghalaya, Shillong, India in 2018. Currently, he is working as Assistant Professor in the Department of Electrical Engineering at the National Institute of Technology Meghalaya, Shillong, India. His current research interests include the PMU estimation algorithms, application of Phasor Measurement Units for wide-area protection and power system dynamics.