Authentication mechanism in converter-based DC network

Sicheng Gong

Abstract—This paper proposes a novel event-triggered attack detection mechanism for multi-agent DC microgrid system. Under a distributive network framework, each node only collects its neighbours' relative data to regulate its own output for inner system stabilization. Hardly can an agent identify the source of unexpected outside power flow directly without power line current data, especially under an organized attack composed of voltage variation and corresponding deceptive messages. In order to recognize traitors who broadcast wrong data, aim for system distortion and even splitting, an efficient attack detection and identification strategy is mandatory. After the attack detector is triggered, each relative agent refuses to trust any received data directly before authentication. During two-step verification by comparing theoretical estimated signals with received ones, both self sensors and neighbour nodes would be inspected, and the attacker was difficult to hide himself only except Buck converters were employed globally. Through simulation on MATLAB/SIMULINK, the effectiveness of proposed detection algorithm has been proved.

Index Terms—Authentication mechanism, attack detection, DC/DC converter, transient wave analysis.

I. INTRODUCTION

DUE to stochastic nature of renewable energy generation (REG), DC interconnection is advantageous for REG-integrated power system as its looser grid code, which merely pays attention to voltage magnitude and owns higher tolerance for system oscillations[1]–[3]. Moreover, integration facility and low conversion loss highlights the necessity of DC system deployment, especially in offshore or railway application scenarios[4], [5]. DC microgrid can be a economical and reliable scheme for REG-integrated power system, and its rapid emergence proves its priority to conventional AC grids[6]–[8]. Nonetheless, without external power regulation or internal topology reconfiguration, the global stability of DC microgrid can still be easily influenced by power imbalance under a limited self regulation capacity, no matter where power perturbation is generated.

In order to improve DC microgrid reliability, there exists a common solution of redundant battery energy storage (BES) embedment for power regulation, which plays an alternative role of external regulator[9]–[11]. However, BES is commonly expensive and only intended for periodic or random power variation[12]. It is impossible to regulate long-term constant power variations considering its finite capacity. Precisely,

under deliberate biased node voltage or accidental node fault, power imbalance in DC microgrid will exist for a long time and BES cannot support for a long time under such attack, until relative nodes are classified and removed actively. Facing potential attack from neighbours and a lack of central controller, attack detection is mandatory for each agent in distribute power system for self protection. The derived attack identification conclusion, as a credible reference for future network top logy reconfiguration, will ensure each node's personal and global stability in final.

A brief survey on attack detection for cyber-physical systems has been conducted in [13], including central controller and distributive controller scenarios in general cyber-physical systems. Regarding distributive power system, a model-based physical attack detection strategy for generation control has been proposed in [14], and intrusion detection in distributed frequency control for microgrid was investigated in [15]. Besides, several model-free methods were discussed to detect false data injection attack in power grid as well, for instance sparse optimization, wavelet transform and deep neural networks[16], [17]. All detection methods above are intended for AC grid, and specific physical properties of DC microgrid should be taken into consideration.

For an emerging converter-dominated DC microgrid, signal temporal logic formalism can be employed to detect attacks and evaluate relative impacts on system stability[18], while it cannot help identify the attack source. In [19], a stealth cyber-attack detection strategy using cooperative vulnerability factors was proposed, while based on a hypothesis that neighbours' output current signals are accessible and trustworthy. A distributed cyber-attack detection scheme using a Luenberger observer has been investigated in [20], while it still relies on two trustworthy nodes. All strategies above cannot realize attack source identification and mere self data utilization in the same time. The motivation of the present work in this paper is to address this challenge.

Event-triggered mechanism can save computation and communication resource in a dynamical system, while still ensuring stable system performance[21]. This paper proposes a novel event-triggered attack detection and identification strategy, utilizing a nonlinear relationship between switcher duty ratio and converter transfer ratio, in order for rapid and accurate attack detection in most scenarios only based on self data. Through transient wave analysis during two-step examinations, no malicious node can hide himself and a reconfigured network topology will remove those nodes eventually.

The rest of this paper is organized as follows. Section II

M.Gong was with the Department of Electrical Engineering, Technical University of Denmark, Lyngby, 2800, Denmark. E-mail: s190027@student.dtu.dk.

This work has been submitted to the IEEE for possible publication. Copyright may be transferred without notice, after which this version may no longer be accessible.

Fig. 1: Simple DC grid case utilizing Buck-Boost converters

represents general structure of DC microgrid, including several hypothesis for future analysis simplification. The detailed categorization of DC microgrid attack has been illustrated in Section III. Then specific attack detection mechanism is explained in Section IV. Simulation and hardware verification are implemented in Section V and a conclusion is provided in Section VI.

II. SYSTEM DESCRIPTION AND MODELING

The configuration of investigated system including subsystem modules and DC transmission lines is shown in Fig. 1(a). Periodic communication between each other is mandatory to come to a power balancing consensus. There are several assumptions employed during strategy investigation, which finally ensure proposed methods' effectiveness.

A. Subsystem module

The subsystem module plays a role of agent in microgrid, who exchanges electric power and gives priority to internal stability guarantee. For modelling simplification, the subsystem is assumed composed of an ideal stable voltage source and a buck-boost converter interface. The converter duty ratio determines node output voltage, finally influencing its neighbours through relative transmission lines.

As switching signals are generated by each agent's own controller, only based on its local and received data. Under a stable power sharing consensus, the duty ratio should be constant and it can only change when receiving other nodes' personal requests or reaching another consensus.

B. Sensor

A complete agent in DC microgrid is composed of a subsystem module and inner sensors. The sensor should be integrated into converter for state monitoring. In industrial scenarios, its sampling frequency is commonly equal or similar to switching frequency, which means there is no possibility of quick duty ratio derivation only depending on sensing data. For further illustration, if the duty ratio changes, no other agent or attacker is unable to find the duty ratio in several switching periods, expect being informed directly by the converter controller. Such prerequisite is fundamental to ensure the validity of proposed attack detection strategy.

A trustworthy inner inductor current sensor in converter is mandatory, or subsystem output power measurement can be an alternative. In accordance with converter topology, these two values can be estimated from each other, and (4) elaborates the calculation in a Buck-Booster converter case. The converter output current can be another alternative likewise. With all internal sensors betrayed simultaneously, the converter controller is assumed blind and even instigated, as its subsystem has broken down and there is no reference for attack source identification even that attack has been detected.

$$I_{Li} = \frac{P_s}{\alpha \cdot U_{Si}} \quad (1)$$

where P_s denotes measured subsystem output power and I_{Li} denotes estimated inner inductor current in node i . α is the duty ratio of switcher near to inner voltage source, and U_{Si} is the inner voltage source output level, estimated according to converter output voltage signals in node i .

If inner voltage source output level was measured and trustworthy as well, there would be no need for converter voltage sensor examination considering their relationship. That explains why only estimated value of U_{Si} is utilized in this paper. The transmission line current sensor is designed discredited in our investigated cases likewise. Actually, with detailed transmission line current data, the attack has no way to hide himself. The attack is only effective only when line current data is inaccessible for attacked nodes.

The trust level and availability of all sensors during attack detection are summarized in Tab I. Three colors indicates three possible and incompatible scenarios. A low trust level denotes relative signals should be authenticated by detector before trust, while signals with high trust level is assumed reliable at any time. If the sensor is available for attack detection, it may be modified deliberately while it cannot be shielded. The so called "unavailable" signal means that it would not be utilized for attack detection, and if it was not shielded, it can still be trusted during normal network communication after attack removal.

TABLE I: Table of sensor during attack detection

Measurement	Trust level	Availability
Converter inner voltage	Low	No/Yes/Yes
Converter output voltage	Low	Yes/No/Yes
Converter inductor current / Subsystem output power / Converter output current	High	Yes
Neighbour output voltage	Low	Yes
Transmission line current	-	No

C. DC Transmission line

The DC transmission line is equivalent to an ideal conducting line, series with a lumped resistor and parallel with ground capacitors on its terminals. For modelling simplification, the terminal ground capacitance can be merged into node output capacitance. Moreover, considering oscillation nature of converter output, a cascade inductor can be added in series with the lumped resistor to ensure high frequency model accuracy.

Fig. 2: DC microgrid attack categories

D. Network topology

The network topology is essential to each node for its own parameter tuning in attack detection strategy. There is no restriction on DC microgrid topology, meaning that each node is able to disconnect or connect with other nodes actively, while each topology reconfiguration should always notify all nodes. The network parameters are assumed trustworthy and accessible for all participants, including topology, relative line impedance and admittance

III. OPERATION PRINCIPLE OF DC MICROGRID ATTACK

The main target of grid attack is to cause a divergence between signal and reality, resulting in massive power imbalance in grid, finally splitting the network or dragging it to another stable point. For further illustration, the grid attack can be categorized into three patterns, as shown in Fig. 2, including signal shielding, signal substitution and agent instigation.

The jammed or substituted signals should be dropped actively for receivers, and a robust local controller should be integrated to the subsystem to ensure its inner stability. Regarding an instigated agent, all innocent neighbour nodes should ignore its commands and isolate the node until external intervention. Similar to re-closing device in relay protection, the system may give another chance to detected evil nodes if it can stand previous disturbance again. Meanwhile, when Sybil attack is detected, an innocent agent is expected to disconnect with DC links initiatively for self protection.

A. Signal shielding

Sensor destruction, cyber link destruction and cyber link jamming are typical attacking methods to shield signals. Without external measurement and communication information, the subsystem module is highly potential to lose physical synchronization with its neighbours under unexpected oscillations.

In communication protocol vulnerability analysis, the jamming attack is frequently discussed, for instance denial of service (DoS) and selective packet delay[22]. Since cyber link jamming may occur as well in normal scenarios, the jamming attack would not trigger external intervene quickly. Meanwhile, direct equipment damage can lead to an opposite situation, which means less space for further attack action. Considering physical destruction is also expensive and risky for attackers, cyber link jamming can be a suitable choice for signal shielding attack.

In accordance with reliability requirement, the subsystem controller should be designed robust even in an extreme scenario with most monitoring data missing. In such scenario,

mere jamming attack can be difficult to influence local or global stability, hence it is commonly combined with other attack options and comes to be efficient and powerful.

B. Signal substitution

Both sensor instigation and message substitution are intended for signal substitution attack, and the latter one includes package manipulation and repetition, which are still expensive to implement due to message authorization mechanism. However, combining with signal shielding, only a few cyber links need to be focused as the system has no choice but to rely on these links for communication.

C. Agent instigation

Byzantine attack and Sybil attack are distinguished from the magnitude of instigated agents[23], [24]. Instead of instigating several nodes in Byzantine attack, Sybil attack indicates a high penetration ratio of traitors. The controlling behavior of these instigated agents will generate and distribute fake information, which means mismatching between its physical behavior and declaration, aiming to tract the system to another state or breakdown.

For further discussion, a node claimed a false voltage level, and its neighbour nodes would decrease their output voltage accordingly. Afterwards, with its actual high voltage, excessive power will flow into those neighbour nodes, finally destabilizing their inner systems and forcing them kicked out of global grid. Such attack methods can also work together with signal shielding, imposing severer impacts on network.

IV. EVENT-TRIGGERED ATTACK DETECTION AND IDENTIFICATION

Signal shielding can be easily detected by any relative agents, while its influence should be mitigated in order to ensure short-term system stability, which will be discussed later. Considering high inertia designed in most systems, temporary power flow distortion resulted from signal shielding can hardly influence global system stability. A cheating attack seems more economical for attackers since it can generate unmatched power flow for a long period, considering such attack is commonly designed to avoid being detected before implementation. That explains why signal shielding is ignored and other two types of attacks are mainly discussed in proposed detection mechanism. The proposed detection flow chart is illustrated in Fig. 3.

An event trigger should be designed based on attack detection, as shown in the blue block in Fig. 3, in order to save computation and communication resource in distributive network. When received neighbour data are estimated incompatible with its own data according to (2), the detector is triggered and attacking pattern will be classified.

$$\hat{I}_{out}^i = \frac{U_i}{z_{ii}} - \sum_{E(i,j) \neq 0 \& i \neq j}^n \frac{U_j - U_i}{z_{ij}} \quad (2)$$

where $\hat{I}_{out}^i$ is the estimate value of output current from node i , U_i is declared voltage level of node i . $E(i, j)$ is a 0/1 variable

B. Neighbour examination

With trustworthy signal from self sensors, evil neighbours should be detected. Active voltage injection can be useful for evil neighbour classification if network impedance matrix is open data. With event of "attack" triggered and active voltage injected, the slope of output/input current variation to voltage variation can be utilized to judge which agent is lying, since different line impedance. As the evil agent has no access to other agents' communication message, with a scheduled synchronized ramping or dropping voltage wave of two agents, the instigated agent can be detected by cross validation.

The principle of evil member classification using voltage injection is explained as follows. In a stable network after some node voltage variation, for a specific node i , its output voltage variation can be calculated in (5), in order to verify the status of a specific neighbour node j . In order to survive, if a node request the attacking node to adjust voltage, the attacker has no choice but to raise or drop its output voltage accordingly in honest, otherwise, unmatched current data will reveal the attacker after the network comes stable.

$$\Delta I_{out}^i = \frac{\Delta U_j}{z_{ij}} \quad (5)$$

For transient analysis to classify the attacker, based on simplified circuits shown in Fig. 1(b), global network state vectors including voltage vector $\mathbf{U}$ and current output vector $\mathbf{I}$ can be written as (6)-(9).

$$\mathbf{I} = \mathbf{Y}\mathbf{U} \quad (6)$$

$$\begin{aligned} \mathbf{U} &= [U_1 \quad \dots \quad U_i \quad \dots \quad U_n]^T \\ \mathbf{I} &= [I_{out}^1 \quad \dots \quad I_{out}^i \quad \dots \quad I_{out}^n]^T \end{aligned} \quad (7)$$

$$Y_{ij} = \begin{cases} -y_{ij} & i \neq j \\ \sum_{k=1}^n y_{ik} & i = j \end{cases} \quad (8)$$

$$y_{ij} = \begin{cases} \frac{1}{z_{ij}} & E(i, j) \neq 0 \\ 0 & E(i, j) = 0 \end{cases} \quad (9)$$

where y_{ij} is the admittance of transmission line between node i and node j . $\mathbf{Y}$ is the admittance matrix of network.

Utilizing each node's output ground capacitor, whose capacitance is denoted as C_i , the impulse current from node who has detected the attack and injected voltage actively, should satisfy a relationship in (10)-(12) in a linear circuit.

$$\begin{aligned} \mathbf{C} &= [C_1 \quad \dots \quad C_i \quad \dots \quad C_n]^T \\ \mathbf{I}_{imp} &= [0 \quad \dots \quad I_{imp}^i \quad \dots \quad 0]^T \end{aligned} \quad (10)$$

$$I_{imp}^i = \Delta \alpha_i \cdot I_{cov}^i = \frac{-\Delta \alpha_i \cdot I_{out}^i}{1 - \alpha_i} \quad (11)$$

$$\frac{\mathbf{I}_{imp}(s) - \mathbf{I}(s)}{s} = \mathbf{C} \circ \mathbf{U}(s) \quad (12)$$

where I_{imp}^i represents impulse current generated by adjusted duty ratio, and I_i represents converters inner inductor current.

$\Delta \alpha_i$ is the variation of duty ratio. $\circ$ means Hadamard product, denoting element-wise product between two matrices.

If Sybil attack happens, such detection mechanism may fail as some evil agents can mask each other through stealth attack. Under such circumstance, voting system for all suspect nodes can perform better while a global ballot ticket collector should be picked. In this paper, this extreme scenario will be neglected as stealth attack is commonly difficult to implement especially with complicated physical behaviour of converters.

Actually, the operation principle in neighbour examination can be applied for self sensor examination and vice versa. The accuracy of transient wave analysis is insensitive to the magnitude of duty ratio variation, while such strategy relies on symbol computation and sets a high standard to node computing capability. The strategy choice depends on attack severity. As no physical damage resulted immediately by self sensor instigation, it allows longer responding time for testing and much computing resource can be saved by transition period estimation. Agent instigation examination is on the contrary.

However, in accordance with detection flow chart in Fig. 3, as self sensor examination is always in advance of agent examination, rapid-response-required part is put afterward, violating original intentions of strategy choice. For industrial application, the order of examination should be exchanged, or let self sensor check be a routine before detection triggered. The procedure order in Fig. 3 is only designed for REG-integrated microgrid, where internal regulating capacity is enough and a quantity of nodes are naturally stochastic and unmanageable generation units, meaning that sensor attack in this network is more cheap and frequent.

C. Network data calibration

With no attacker identified in previous two procedures, node fault should be checked first. However, relay protection is commonly integrated and operates immediately when node fault happens. The step of node fault is illustrated by dashed line in Fig. 3, meaning that it may be dropped in most industrial application as relay protection requirement, and may be kept if some minor faults won't trigger relay protector and still needs to be removed in future. If no attack or fault happen, the network parameter data $\mathbf{Y}$ and $\mathbf{C}$ should be calibrated based on inverse calculation using (6)-(12).

V. VALIDATION AND DISCUSSION

The theoretical solution for attack detection to distinguish attack category has been illustrated. In order to verify the validity of proposed method, both simulation test on MATLAB/SIMULINK and hardware test on dSpace platform have been implemented. Detailed discussion were provided when comparing theoretical solutions with experimental data, and the efficacy of proposed method was proven.

A. Simulation verification

Regarding a simplified 4-node MVDC microgrid shown in Fig. 4, buck-boost converters are employed as interfaces connecting inner system to neighbour nodes. The parameters of simulation system are listed in Tab. II.

Fig. 4: Schematic of DC microgrid case

TABLE II: Table of simulation system parameters

Parameter	Value	Meaning
f_{sw}	10kHz	Switching Frequency
R_{line}	2 Ω	Power line equivalent series resistance
L_{line}	5mH	Power line equivalent series inductance
R_{load}	64 Ω	Load resistance
V_{in}	800V	Subsystem input voltage
C	500 μ F	Subsystem output ground capacitance
L	0.2H	Inner inductance in converter
D	0.5	Expected duty ratio of switcher near to input power source

Fig. 5: Mathematical and simulation samples of U and $\frac{\partial U}{\partial t}$

1) *Agent instigation detection*: In this paper, Node 2 was picked as an instigated agent to attack the global grid, who tried to steal energy from grid and tract it to a lower voltage level. Through adjusting its relative duty ratio to 0.4, its neighbour node 1 would send a voltage adjustment request after self sensor verification. A further illustration to nodes' interaction mechanism has been given in Fig. 3. Node 2 had no choice but to adjust voltage accordingly, while the mismatched output voltage data of Node 1 would reveal Node 2's guilty.

From the perspective of Node 1, whether Node 2 was cheating, it can generate theoretical solution to estimate its future voltage variation after relative nodes' action, as shown in orange lines in Fig. 5a. The mathematical solution of Node 1 voltage derivative could be derived as orange lines Fig. 5b show. Meanwhile, the relative simulation results of Node 1 output voltage in both scenarios are given in blue lines in Fig. 5a-5b. If a specific scenario has been assumed, the large divergence between theoretical solution and sampled data would help prove or reject the assumption. Detailed simulation results regarding output voltage waves of Node 1 are given in Fig. 6. Moreover, it is concluded that the theoretical and simulation results highly matched for the same scenario.

Fig. 6: Detailed wave of U in Node 1

VI. CONCLUSION

The proposed detection method has been verified by simulation, while nonlinear equipment in microgrid can cause a big confuse during attack identification. More investigation on complicated scenarios should be implemented in future.

ACKNOWLEDGMENT

The authors would like to thank the PowerLab DK in DTU for hardware test support.

REFERENCES

- [1] P. Sanjeev, N. P. Padhy, and P. Agarwal, "Peak energy management using renewable integrated dc microgrid," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4906–4917, 2017.
- [2] A. T. Elsayed, A. A. Mohamed, and O. A. Mohammed, "Dc microgrids and distribution systems: An overview," *Electric power systems research*, vol. 119, pp. 407–417, 2015.
- [3] J. J. Justo, F. Mwasilu, J. Lee, and J.-W. Jung, "Ac-microgrids versus dc-microgrids with distributed energy resources: A review," *Renewable and sustainable energy reviews*, vol. 24, pp. 387–405, 2013.
- [4] N. Holtsmark, H. J. Bahrat, M. Molinas, B. A. Mork, and H. K. Hoidalén, "An all-dc offshore wind farm with series-connected turbines: An alternative to the classical parallel ac model?" *IEEE Transactions on industrial Electronics*, vol. 60, no. 6, pp. 2420–2428, 2012.
- [5] F. Perez, A. Iovine, G. Damm, L. Galai-Dol, and P. F. Ribeiro, "Stability analysis of a dc microgrid for a smart railway station integrating renewable sources," *IEEE Transactions on Control Systems Technology*, 2019.
- [6] N. Ertugrul and D. Abbott, "Dc is the future," *Proceedings of the IEEE*, vol. 108, no. 5, pp. 615–624, 2020.
- [7] McKinsey. (2010). "ransformation of Europe's power system until 2050," [Online]. Available: https://www.mckinsey.com/~media/mckinsey/dotcom/client_service/epng/pdfs/transformation_of_europes_power_system.ashx (visited on 10/17/2020).
- [8] H. A. P. Grids. (2020). "Hitachi ABB Power Grids launches game-changing EV charging system for large scale e-Mobility," [Online]. Available: <https://www.hitachiabb-powergrids.com/news/global-news/press-releases/hitachi-abb-powergrids-launches-game-changing-ev-charging-syste> (visited on 07/15/2020).
- [9] J. Zhou, M. Shi, Y. Chen, X. Chen, J. Wen, and H. He, "A novel secondary optimal control for multiple battery energy storages in a dc microgrid," *IEEE Transactions on Smart Grid*, 2020.
- [10] J. Sun, W. Lin, M. Hong, and K. A. Loparo, "Voltage regulation of dc-microgrid with pv and battery," *IEEE Transactions on Smart Grid*, 2020.
- [11] T. Morstyn, A. V. Savkin, B. Hredzak, and V. G. Agelidis, "Multi-agent sliding mode control for state of charge balancing between battery energy storage systems distributed in a dc microgrid," *IEEE Transactions on smart grid*, vol. 9, no. 5, pp. 4735–4743, 2017.
- [12] L.-Y. L. Hsieh, M. S. Pan, Y.-M. Chiang, and W. H. Green, "Learning only buys you so much: Practical limits on battery price reduction," *Applied Energy*, vol. 239, pp. 218–224, 2019.
- [13] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, "Brief survey on attack detection methods for cyber-physical systems," *IEEE Systems Journal*, 2020.
- [14] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.
- [15] L.-Y. Lu, H. J. Liu, H. Zhu, and C.-C. Chu, "Intrusion detection in distributed frequency control of isolated microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6502–6515, 2019.

- [16] J. James, Y. Hou, and V. O. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3271–3280, 2018.
- [17] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.
- [18] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3585–3595, 2018.
- [19] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.
- [20] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to dc microgrids," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3800–3815, 2020.
- [21] L. Ding, Q.-L. Han, X. Ge, and X.-M. Zhang, "An overview of recent advances in event-triggered consensus of multiagent systems," *IEEE transactions on cybernetics*, vol. 48, no. 4, pp. 1110–1123, 2017.
- [22] B. Moussa, M. Debbabi, and C. Assi, "Security assessment of time synchronization mechanisms for the smart grid," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1952–1973, 2016.
- [23] A. Geetha and N. Sreenath, "Byzantine attacks and its security measures in mobile adhoc networks," *Int'l Journal of Computing, Communications and Instrumentation Engineering (IJCCIE 2016)*, vol. 3, no. 1, pp. 42–47, 2016.
- [24] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*, Springer, 2002, pp. 251–260.
- [25] B. Ismaiel, M. Abolhasan, W. Ni, D. Smith, D. Franklin, and A. Jamalipour, "Analysis of effective capacity and throughput of polling-based device-to-device networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8656–8666, 2018.
- [26] S. S. Hussain, T. S. Ustun, and A. Kalam, "A review of iec 62351 security mechanisms for iec 61850 message exchanges," *IEEE Transactions on Industrial Informatics*, 2019.
- [27] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of Network and computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.