Centralized Volt–Var Optimization Strategy Considering Malicious Attack on Distributed Energy Resources Control

Ankur Majumdar, *Member, IEEE*, Yashodhan P. Agalgaonkar, *Member, IEEE*, Bikash C. Pal 🆔 , *Fellow, IEEE*, and Ralph Gottschalg 🆔 , *Member, IEEE*

Abstract—The adoption of information and communication technology based centralized volt–var control (VVC) leads to an optimal operation of a distribution feeder. However, it also poses a challenge that an adversary can tamper with the metered data and, thus, can render the VVC action ineffective. Distribution system state estimation (DSSE) acts as a backbone of centralized VVC. Distributed energy resources (DER) injection measurements constitute leverage measurements from a DSSE point of view. This paper proposes two solutions as a volt–var optimization DSSE malicious attack mitigating strategy when the DER injection measurements are compromised. The first solution is based on local voltage regulation controller set-points. The other solution effectively employs historical data or forecast information. The concept is based on a cumulant-based probabilistic optimal power flow with the objective of minimizing the expectation of total power losses. The effectiveness of the approach is performed on the 95-bus U.K. generic distribution system and validated against Monte Carlo simulations.

Index Terms—Bad data detection (BDD), distributed energy resources (DER), malicious attacks, volt var optimization (VVO).

I. Introduction

MODERN power systems are rapidly integrating growing capacity of renewable generations. The proportion of solar generation in present generation portfolio mix is steadily increasing. UK is scheduled to have 22GW of installed capacity of solar by 2020 [1]. With the increased adoption of such distributed energy resources (DERs), there is going to be a paradigm shift of monitoring, control and operation functions of the distribution network. For its reliable operation, power distribution network operator (DNO) needs to operate the system
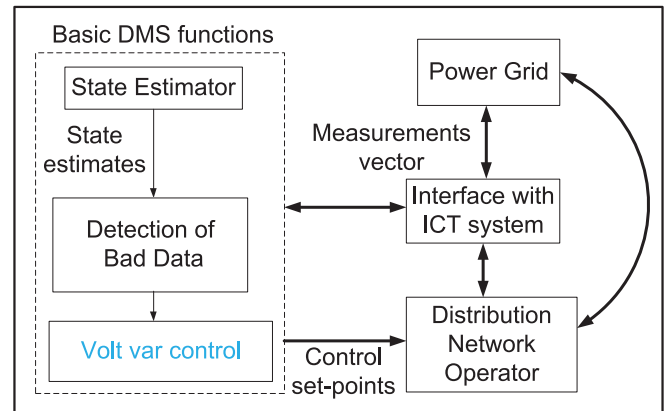
Fig. 1.   A typical distribution management system architecture.

in an optimal manner [2]. In order to achieve this, it is required to control the different components of the network by a massive exchange of data from the smart meters, photovoltaic (PV) inverters to the control center and vice versa through the communication network. This exposes the operation of the network to malicious attacks from adversaries. Such data tampering will affect the control functions of the distribution management system (DMS) such as integrated volt var control (VVC) and thus, resulting into less reliable and efficient operation of the network [3]–[5].

VVC is an integral part of modern distribution management system. A typical DMS architecture shown in Fig. 1 illustrates that. The accurate estimation of the states is essential to enable effective control of the distribution feeder. Based on the estimated states the DMS runs a volt var optimization algorithm to determine the optimal control set-points of the system. These set-points are typically voltage, on load tap changer (OLTC) set-points, and PV inverter reactive injection settings etc. The DNO takes its decisions based on the optimal control set-points.

With the increase in PV uptake the distribution system will face the inherent challenge of voltage rise issue [6]. From a DNO perspective, the voltages at all the feeder nodes are desired to be within the operational limits. The voltage control devices i.e. OLTC, voltage regulators, capacitor banks etc. ensure that the voltages are maintained within limits [7]. Conventionally, the PVs have been operated at unity power factor [8]. In that

situation, the overvoltage is curbed by PV active power curtailment. However, under the draft revised IEEE Standard 1547.8, the PVs are allowed to participate in the voltage and var control through reactive power support and active power regulation. This necessitates over-sizing of PV inverters [9], [10]. The transformer tap changers, voltage regulators, PV inverters need to coordinate with each other through communication network for a centralized VVC [11]. The two-way communication based smart grid voltage control has been proposed in [12]. Most of the other recent works have also devised communication based supervisory control to address these challenges [13], [14].

Unlike in transmission systems, the state estimation is not run in distribution systems very routinely and in real time. Moreover, even the modern smart meter data are not communicated to the supervisory control and data acquisition system (SCADA) or DMS so often [15], [16]. Should there be a bad or erroneous measurement, the bad data detection algorithm identifies and eliminates that. However, in situations where the leverage measurements – those significantly influence the final state estimates – are compromised, it is not feasible to eliminate those faulty measurements. Even with the presence of bad data in leverage measurements the decision for volt var control has to be taken immediately.

Traditionally, the bad data detection has been carried out by largest normalized residuals, χ^2 test, placement of time synchronized phasor measurement units (PMUs) [17]–[19]. Recently published research [20] has addressed the bad data detection in the context of leverage point attacks. However, attacking the leverage measurements is the worst possible form as eliminating those measurements would have a significant influence on the final estimates of the system [21]. The observability of the network and the state estimation is improved by measurement placement [22]. But, this is not useful in real-time decision making. Hence, this provides the motivation to have a real-time decision making process when the tampered leverage measurements are detected.

In recent years, the research focus has shifted towards the security of smart distribution systems such as against attacks on volt var control systems. Teixeira et al. [3] have discussed about integrity attacks on volt var control and proposed a game theoretic approach to counter these attacks. However, they have not considered PV systems in their framework. Reference [5] have assessed the security of the system under DER node compromises in a radial system with no reverse power flow. Reference [4] has discussed the cyber attacks on voltage control with PVs on a radial system. However, none of them have addressed the scenario when the leverage PV injection measurements are attacked. To the best of our knowledge, this paper, for the first time, proposes a optimization strategy to address the issue in real-time.

The paper is structured as follows – Section II discusses the possible attack strategies to influence the measurements and gives a brief description of bad data detection techniques. Section III explains in detail the proposed approach for the volt var optimization strategy. Section IV presents a case study and detailed discussion of the results. The method has been tested on the UKGDS 95-bus system. The concluding Section V provides a summary of the specific contributions of the work.
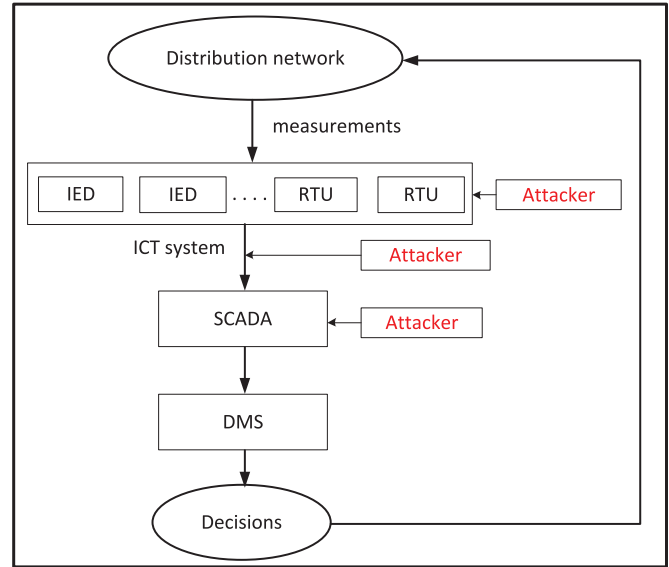

Fig. 2.   Attacks at various levels of distribution system.

II. ATTACKS AND BAD DATA DETECTION

A. Cyber Attacks and Attack Scenarios

The VVC is carried out in two ways – centralized control and distributed control. In distributed control, the whole big problem is sub-divided into many smaller sub-problems. This makes the computation faster. However, since there is no master controller, it is not possible to achieve an optimal operation. In centralized control, on the other hand, the master controller in the DMS processes all the information from the slaves and thus, helps to achieve the optimal control set-points. It utilizes the ICT infrastructure to transmit measurements and also to transmit optimal set-points back to voltage control devices. This makes the centralized control particularly vulnerable to compromises from the attackers.

An attacker can influence the measurements in the system at various levels as shown in Fig. 2. The attacker either corrupts the measurements by attacking through the remote terminal units (RTUs), or by breaking into the system through the communication network or by tampering with the SCADA system through the local area network. Besides, a PV owner for his own profit may also tamper with the meter in order to show that it produced more solar power.

The attacker needs to manipulate a number of measurements to make an attack successful. However, if the measurement is a critical or leverage and not protected then the attacker is required to falsify only that measurement [21]. This falsification of leverage measurements leads to inaccurate estimation of the states and in this situation, the VVC becomes vulnerable. The distribution network, spread across a vast geographical region, is scheduled to host PVs even in remote locations. Hence, a PV power injection measurement has a high chance of being a leverage measurement. This has provided the basis of formulating the attack scenario when the PV nodal injection measurements are compromised.

Though PV is considered, here, as an example this attack scenario is relevant to any other DER or any other leverage
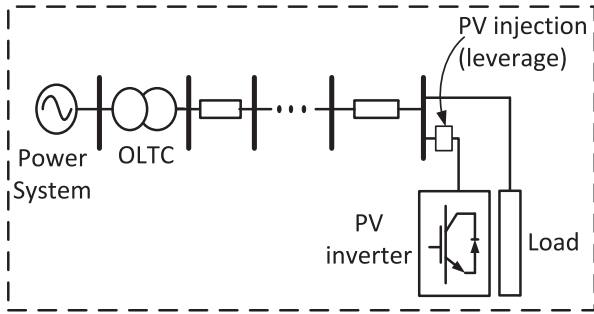
Fig. 3.   The PV injection as leverage measurements.

measurement. A nodal power injection is a *leverage* measurement point, if there are multiple branches connected to that node. Also, a nodal power injection is a *leverage* measurement if one of the branch impedances connected to it is quite different from the other one. As a result, the number of non-zero elements in the Jacobian matrix will be more than the others. In state estimation methodology, the estimated measurement vector is defined as

$$\Delta \hat{z} = K \Delta z \qquad (1)$$

where, z is the measurement vector and K is the hat matrix. A leverage measurement will have a large value in the corresponding diagonal element of this hat matrix and thus, will have more leverage or influence on the estimates than others. An attacker can make changes to the particular diagonal elements of the hat matrix to make the attack successful. The details of the attack strategy is given in [20].

B. Detection of Bad Measurement Data

Fig. 3 shows a generic representation of a realistic network. It has PV and OLTC as voltage control devices. The PV inverter and the load are connected to the grid at the point of common coupling. The PV along with its inverter is capable of controlling reactive power at the point of common coupling within the operational limits of 0.95 leading or lagging power factor. The figure also illustrates the possibility of PV injection measurement at the PV node to be a leverage measurement. If the PVs are at the terminal end of a feeder their injection measurements will have significant influence on the final estimates of the states. An attacker with malicious intentions would exploit such vulnerabilities of the network to subvert control functionality of the network.

Prior to VVC, the DNO detects the tampered measurement by the bad data detection (BDD) algorithm. Literature shows that there has been significant research on the bad data detection techniques employed. The largest normal residuals, χ^2 test and others are some of the techniques [17]–[19]. However, these techniques fail if multiple leverage measurements are attacked. The DRGP-GSR technique proposed in [20] shows how to detect bad data when the leverage measurements are attacked. The diagnostic robust generalized potential (DRGP) technique separates the measurement set into two sets of leverage and non-leverage sets. This nullifies the effect of masking/swamping. The

generalized studentized residual (GSR) of each measurements in each set then detects the erroneous measurements, if any. The measurements with bad data will have GSR values more than the cut-off.

After the identification of bad data, the subsequent optimal set-point calculation has to be carried out. How to calculate VVC set-points and maintain efficacy of the VVC in the presence of detected bad data is discussed in the following section.

III. VOLT VAR OPTIMIZATION STRATEGY WITH BAD DATA

In case of situations where bad data are detected, one would settle for the sub-optimal solution. However, for the reliable and effective operation of the distribution network, the distribution network operator needs to obtain the optimal control set points i.e. OLTC secondary voltage and PV inverter set-points. The volt var control is thus formulated here as a stochastic optimization problem. The OLTC secondary voltage and PV inverter voltages are the control variables and the stochastic nature is associated with the PV output and load demand.

A. Problem Formulation

The problem is formulated as a probabilistic optimal power flow (OPF). The objective of the DNO is to minimize the operational losses of the system. But, in the probabilistic sense, it is the expectation of the losses which needed to be minimized.

$$\text{minimize} \quad E_f(P_{\text{loss}}) \qquad (2)$$

where, P_{loss} is the total loss of the system.

The minimization objective is constrained by many operational and system constraints. These are enumerated and explained below:

1) Voltage Constraints: For voltage control the main objective is to maintain the voltage of the system at different nodes within operational limits. This limit is within $\pm 5\%$ of the nominal voltage. Hence, in the probabilistic sense, the probability of bus voltage V to be within the limits should be as high as possible.

$$\text{Prob}\,(V \leq V_{\text{max},l}) \geq \beta_{V,\text{max}} \qquad (3)$$

$$\text{Prob}\,(V \geq V_{\text{min},l}) \geq \beta_{V,\text{min}} \qquad (4)$$

These acceptance probabilities $\beta_{V,\text{max}}$ and $\beta_{V,\text{min}}$ are generally 95%. $V_{\text{max},l}$ and $V_{\text{min},l}$ are the voltage limits.

2) Branch Current Flow Limits: The current flowing through the branches is limited by their thermal capacities. The probability of current I to be outside the limits should be less than 5%.

$$\text{Prob}(I \leq I_{\text{max},l}) \geq \beta_I \qquad (5)$$

where, $I_{\text{max},l}$ is the thermal capacity limit.

3) Solar PV Inverter Limits: To maximize the revenue from PV, the owners would like to operate the PV at maximum power point tracking control. It will be financially attractive to PV owners to curtail active output as less as possible. Therefore,

$$E_f(P_{\text{curt}}) \leq \eta_{\text{curt}} \qquad (6)$$

where, P_{curt} is the curtailed active power.

The reactive power support from the PV inverters is limited by inverter over-capacity limit. Mathematically,

$$\text{Prob}((P_s^2 + Q_s^2) > S_{\text{inv}}) \leq \beta_s \tag{7}$$

where, P_s, Q_s are the active power and reactive power outputs from solar and S_{inv} is the PV inverter capacity.

4) Power Balance Constraint: At each node, the active and reactive power must satisfy the equality constraints. The total power injected at each node must be equal to the difference of generated power and load power. The detailed modelling is carried out as given in [23], [24].

5) Tap Operation Limits: The OLTC in the substation is equipped with taps to participate in voltage control. The OLTC is, however, limited by the tap operational limits. Generally, the OLTC tap positions in the distribution system are generally within ± 16. In other words, there are only 33 tap positions possible. Hence, the probability of voltage at the secondary of the transformer to be within the upper and lower limits should be more than 95%.

$$\text{Prob}(V_t \leq V_{t_{\max,l}}) \geq \beta_{t,\max} \tag{8}$$

$$\text{Prob}(V_t \geq V_{t_{\min,l}}) \geq \beta_{t,\min} \tag{9}$$

where, $V_{t_{\max,l}}$ and $V_{t_{\min,l}}$ are the voltage limits for the substation secondary bus and $\beta_{t,\max}$ and $\beta_{t,\min}$ are the corresponding acceptance probabilities.

B. Mitigation of Malicious Attacks

Once the bad data is detected by the DRGP-GSR methodology, as discussed in Section II, the DNO needs to mitigate the effect of bad leverage data without eliminating them. Considering the fact that the state estimation is not run in less than 15 minutes interval, with the wrong set of state estimates the volt var control would be erroneous.

A decision needs to be taken based on the faulty data and rescheduling needs to be done. As a result, a real time probabilistic volt var control is proposed, here, as a remedy to this. In order to have a prompt and fast decision, the DNO has four things at its disposal. These are – the historical measurement data, historical demand profile, historical solar output profile, and forecast of load and solar output. Based on these historical data the probability distribution curves of each demand and solar output are constructed. With the change in historical data in 5 minute time horizon, the probability density curves are updated as well. The DNO then runs an optimization every 5 minutes with voltage at the secondary of the transformer as one of the variables. The taps, however, are re-evaluated in every 30 minutes. The DNO would, in the end, settle for the statistical mean of the system variables from this probabilistic optimal power flow. However, in the worst case, when the system security is at stake the DNO settles for the sub-optimal solution based on local conditions. The adopted mitigation strategy to alleviate the effect of malicious attacks is illustrated in Fig. 4. It is further described below:

1) Cyber Attack Mitigating Stochastic Optimal Solution (CAMSOS): This remedy is based on coordinated control of
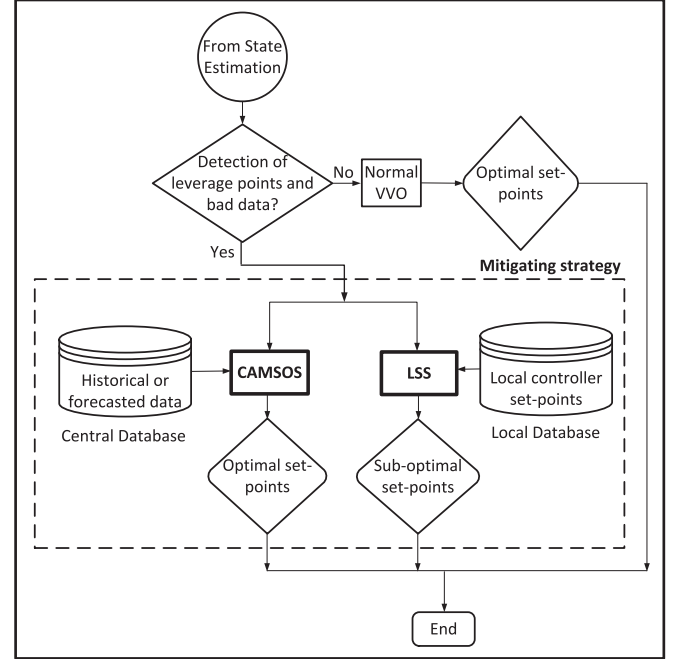

Fig. 4. VVO with malicious attack mitigation strategy.

the voltage and reactive power in the network with an objective of minimizing the active power losses in a stochastic sense. The optimal reactive power dispatch is based on either historical load and PV output data of high granularity (1-sec) or on forecasted load and PV output. The probability distribution curves are generated from these data. However, the decision to adopt historical or forecasted data will depend on the DNO. The DNO will choose the one with lesser variance and this will assist in getting a better optimal solution. The optimal power flow formulation, introduced in the previous subsection, is a stochastic one, which is carried out by cumulant based probabilistic volt var optimization (CPVVO) – a combined logarithmic barrier primal dual interior point and cumulant based method.

The inequality constraints are converted to equality constraints by non-negative slack variables sl. The details of the method are given in [25].

At the optimal solution, the derivative (gradient) of the Lagrangian is zero. This is known as the Karush-Kuhn-Tucker (KKT) condition. To achieve this, all the non-linear equations are linearized around the operating point by Taylor's theorem. Then at each iteration, the state variables are updated based on Newton's step which is given below:

$$H_s(x)\Delta x = -\nabla L(x) \tag{10}$$

where,

x: The vector of state variables

$H_s(x)$: The Hessian matrix

$\nabla L(x)$: The gradient or derivative of the Lagrangian

The solution of the above Newton step in (10) at each iteration is then carried out by cumulant based probabilistic optimal power flow [26], [27]. The stochasticity is due to the randomness of some or all of the variables. The random parameters

considered here are the loads at different nodes and the PV output. The randomness is characterised by some known or unknown distribution functions known as probability density functions (pdf) from historical or forecasted data. The Gaussian mixture model (GMM) of the pdfs is formed, thereafter. The cumulant is a logarithm of the Laplace transform of the original random variable. By linearity property, the nth order cumulants are given by

$$(C_{\Delta x, n}) = -(H^{-1}).^n C_{\nabla L(x), n} \tag{11}$$

Once the cumulants of the output variables (voltage and taps) are obtained they are converted back to pdfs by Cornish-Fisher or Gram-Charlier [28], [29] expansion functions. The detailed steps of the cumulant method are given as below:

1) Calculate the statistical moments of injected power from the distribution functions of loads and PV output
2) Calculate the cumulants of injected power from the moments
3) Compute the cumulants upto 9th order of the state variables from the Newton step
4) Calculate the Cornish-Fisher expansion coefficients from the cumulants and moments
5) The pdf and cdf of the state variables are obtained from the cumulants by the expansion function

Once the pdf and cdfs of state variables are reconstructed, the statistical step, which is the difference between the current value and the peak value, for each variable is computed. Each variable is then updated for the next iteration according to

$$\Delta x = \alpha(w_1 \Delta x_{\text{Newton}} + w_2 \Delta x_{\text{statistical}}) \tag{12}$$

where, α is the step length parameter and w_1 and w_2 are weights associated with each incremental step. The procedure is continued for the next iterations until convergence. Fig. 5 zooms a part of Fig. 4 showing the detailed CAMSOS procedure proposed here.

2) Local Setting Solution (LSS): As a secondary backup, this remedy is resorted to based on the local control of the voltage control devices. The PV inverters and substation OLTCs are equipped with their own controllers. It means that once the bad data is detected, the coordinated control of the network is relinquished and the devices are allowed to operate based on their own local controller settings. In order to maintain the voltages within operating limits, the PV inverter control set-points are reset to local controller settings and the substation OLTC to pre-determined set-points. In this case, system voltage control is achieved by designing set-points for the worst case scenario. Two worst case scenarios are considered – maximum output of the PV generator under low load demand and maximum load demand with low PV generation. Non-coordinated operation of OLTC, VR and PV plant is considered. Only the primary objective of maintaining the system voltage at all the buses is considered and set-points are calculated. Since, the set-points are not based on any objective function, the solution is not optimal and the active power losses may not always be minimized.
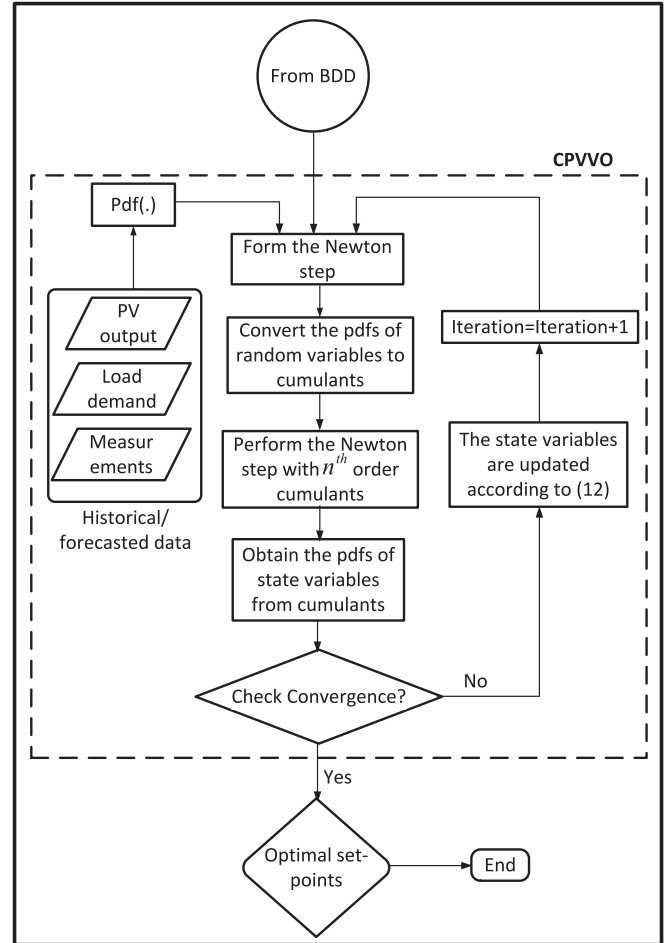

Fig. 5. Cyber attack mitigating stochastic optimal solution.

IV. RESULTS AND DISCUSSIONS

The 95 bus UK generic distribution system (UKGDS) is shown in Fig. 6. It is a 33/11kV system. There are two solar PV plants, each of 1 MW capacity, on bus 18 and bus 89. According to G83/G59 Engineering recommendation [30], [31], the PV inverters are over-sized to allow them to operate upto 0.95 lag/lead pf. The line data and load data for the system are obtained from [32] and the daily load profile with four different kinds of customers has been generated by load profile indices as mentioned there. The solar output profile is generated from the 1-second resolution data at UK Power Networks (UKPN), UK taken in the month of June, 2014. The solar output profile and load demand profile are shown in Fig. 7 and Fig. 8 respectively. The PV is assumed to operate as a static synchronous compensator (STATCOM) at night and thus provides reactive power support. The load distribution and solar distribution curves are generated from their historical data.

There is one OLTC in the substation. The two solar PVs are placed at the ends of two feeders. This makes the PV injection measurements leverage ones.

The proposed algorithm is studied for the following two cases. The cases are so chosen such that the possibility of voltage violation will be high.
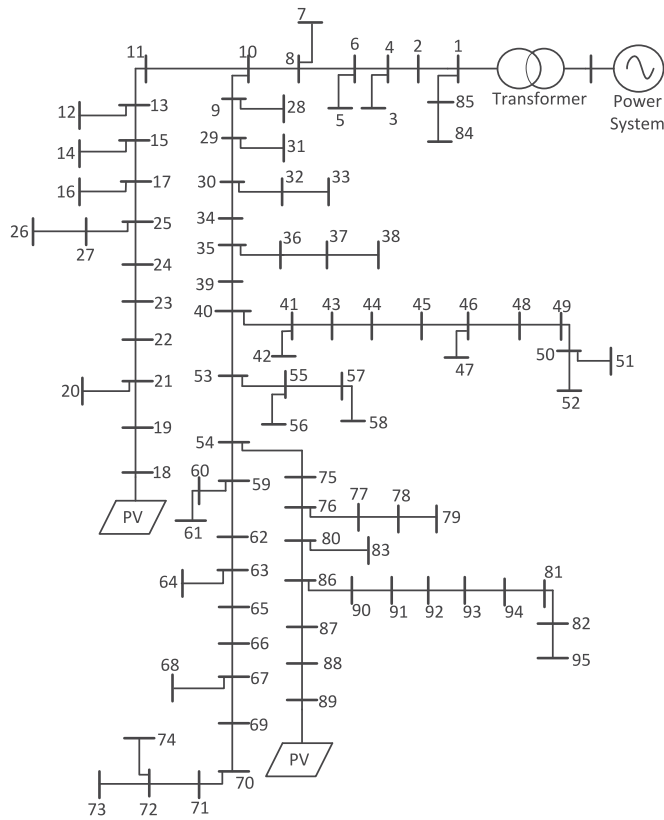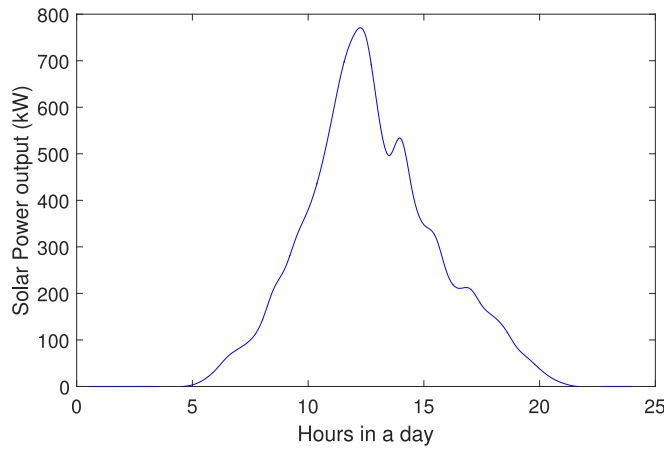
Fig. 6. The 95 node generic distribution system.

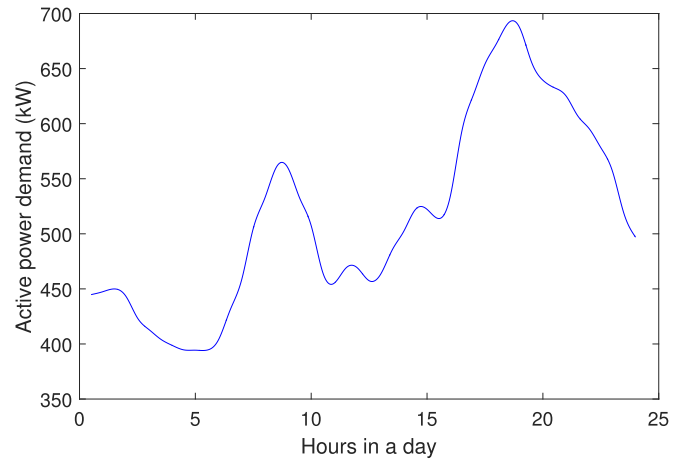
Fig. 7. The PV power output profile in a day.

Fig. 8. The daily active power demand profile of the ukgds system.

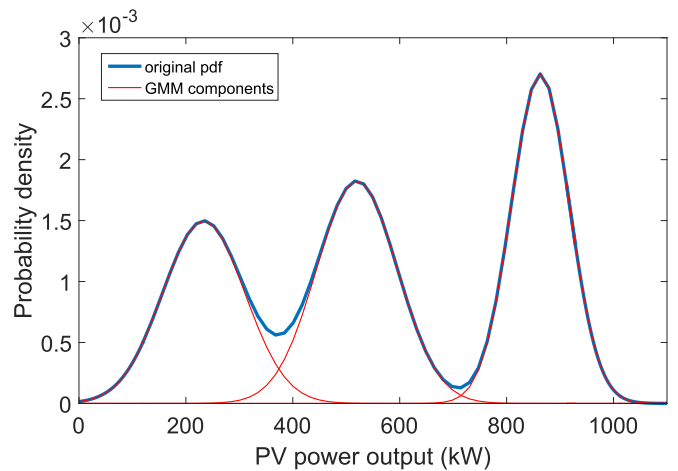Fig. 9. Probability distribution of solar active power output at 12 pm.
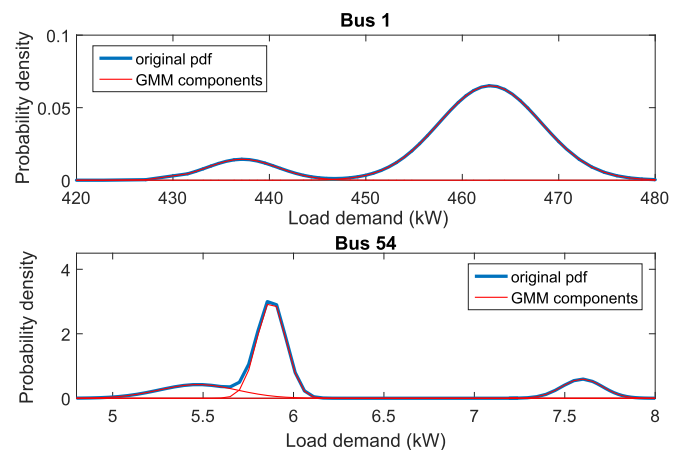
Fig. 10. Probability distribution of load demand at 12 pm.

A. Case1: At Peak Solar Power Output

In this case, the PV power output is at its peak. Normally, in the month of June, the peak occurs at around 12 pm. At that time, the demand is relatively low. The state estimator is run and bad data detector detects the solar PV power injection at node 89 as bad data. The probability distribution curves are generated from the historical PV and load demand data at 12 pm for the month of June. Figs. 9 and 10 show the distribution curves and their Gaussian mixture components. The statistical moments, central moments and cumulants up to 9th order are generated from the distribution curve. The probabilistic op-timal power flow, as described in Section III, is carried out. After convergence, the cumulants of PV inverter voltage set-points are converted back to their probability density functions. The results of the probabilistic OPF is shown in a boxplot in Fig. 11. The boxplot indicates that the voltages at both the nodes
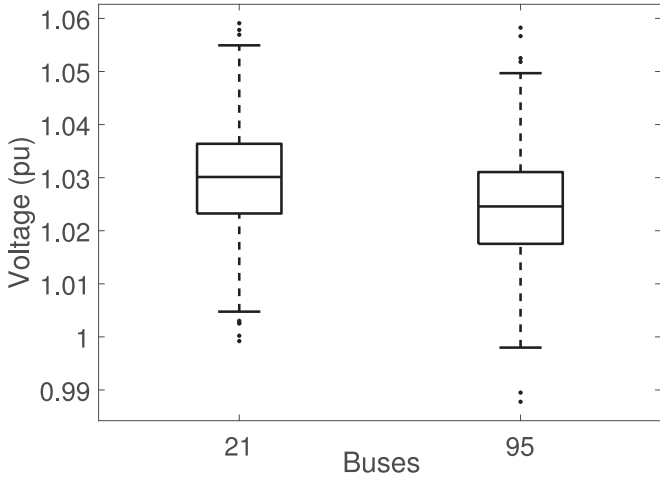
Fig. 11.   Boxplot of voltages of buses for Case 1.

Fig. 12.   Probability distribution of solar active power output at 7 pm.

TABLE I
% IMPROVEMENT IN MEAN AND VARIANCE FOR CASE 1

Variables	Proposed cumulant based method compared with MCS	
	% improvement in mean	% improvement in variance
Voltage	0.9%	3.44%
Angle	1.6%	4.76%
Active power	1.46%	4.85%
Reactive power	1.56%	4.97%

TABLE II
OPTIMAL SET POINTS FOR PV AND OLTC IN CASE 1

OLTC secondary	1.0125
Bus 18	1.029
Bus 89	1.025

Fig. 13.   Probability distribution of load demand at 7 pm.

TABLE III
% IMPROVEMENT IN MEAN AND VARIANCE FOR CASE 2

Variables	Proposed cumulant based method compared with MCS	
	% improvement in mean	% improvement in variance
Voltage	1.2%	4.86%
Angle	1.86%	4.47%
Active power	1.76%	5.49%
Reactive power	1.65%	5.15%

are not violated. Table I further shows the improvement in the mean and variance of the variables according to the proposed method. It has been compared with the mean and variance of a 1500-sample Monte Carlo simulation (MCS). The mean values of the distributions from the cumulant based method are generally within 1% of the mean values from Monte Carlo simulations. The optimal set-points generated from the OPF are shown in Table II.

B. Case2: At Peak Load Demand

In this case, the load demand is at its peak. Usually, the load demand occurs at around 7 pm in the evening but then, the solar output is relatively low. Here also, the tampered data is detected in the PV injection measurement at node 89. The solar power output and load distribution curves and their Gaussian mixture components at 7 pm in the month of June are shown in Figs. 12 and 13. The statistical moment and cumulants up to 9th order are generated from the pdfs. After the probabilistic OPF converges, the pdfs of the voltages are generated. Similar to Case 1, the
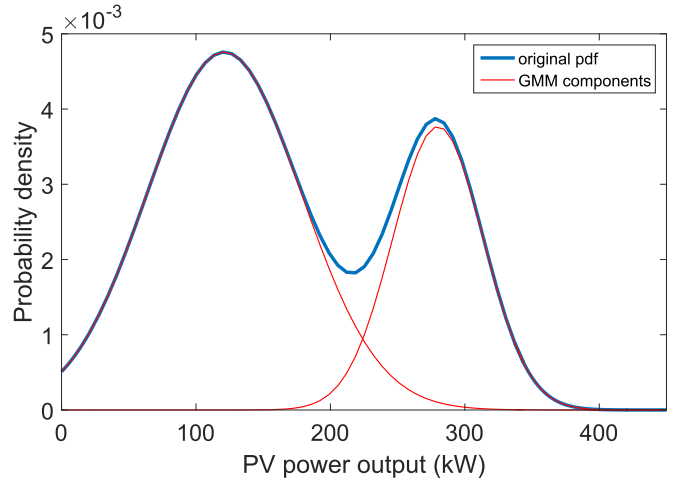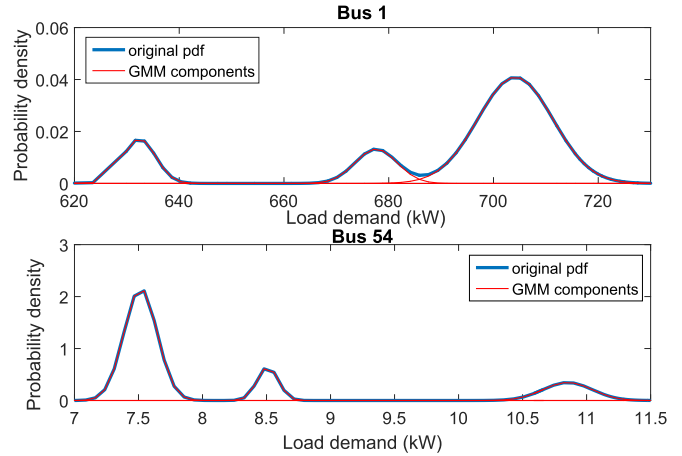
improvement in the mean and variance of the variables compared with that of a 1500-sample Monte Carlo simulation is shown in Table III. The boxplot in Fig. 14 further proves that the voltage remain within limits throughout the process. The optimal set-points are given in Table IV.

The algorithm is coded in Matlab and run on a computer with Intel Xeon processor @3.33 GHz and 12 GB RAM. The proposed method minimizes the operational losses in the system. Table V presents the expectation of losses in both Case 1 and Case 2. The algorithm converges in less than 1 minute. This
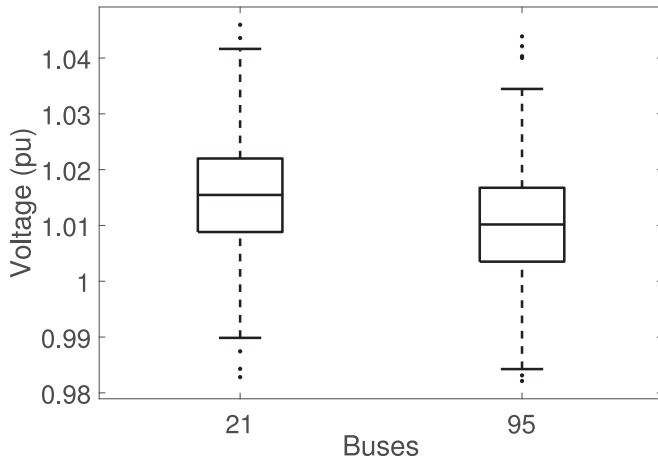
Fig. 14.   Boxplot of voltages of buses for Case 2.

TABLE IV
OPTIMAL SET POINTS FOR PV AND OLTC IN CASE 2

OLTC secondary	1.00625
Bus 18	1.016
Bus 89	1.011

TABLE V
EXPECTATION OF LOSSES

	$E(P_{\text{loss}})$
Case 1	9.45 kW
Case 2	9.24 kW

enables the network operator to take prompt and quick control decisions. The proposed method is studied for two extreme test cases – when the solar output is at its peak and the demand is low and when the demand is at its peak and solar output is relatively low. The month of June is so chosen as the solar output is quite variable in the month of June in the UK. The results for both cases justify that the approach works effectively to obtain the optimal set-points and at the same time minimizes the losses. This further shows that the proposed approach will work for all the other cases of load and PV output and their variability through a day.

V.   CONCLUSION

Due to the utilization of the communication network for the network control, the distribution systems of today are vulnerable. An adversary, who has knowledge about the power system, makes compromises to the network and thus, hampers the effective volt var control. The adversary will choose to tamper with the leverage measurements ensuring failed state estimation and non-operational VVC. The DER injection measurements, which are leverage measurements, are especially prone to these attacks. This paper has proposed two solutions to tackle this scenario. These two solutions are cyber attack mitigating stochastic optimal solution (CAMSOS) and local setting solution (LSS).

It is necessary to estimate the states of the system and detect the bad measurement data. The DRGP-GSR method detects the bad data when the DER injection (high leverage points) measurements are attacked. Once the bad data is detected, rather than utilizing these states their probability density functions are utilized. The CAMSOS proposes utilization of DER power generation and load forecast probability density functions, if these measurements are attacked. Another approach available for CAMSOS is to make use of the historical measurements to compute probability density function of the state which is attacked. The stochastic optimal power flow calculates the voltage control device set-points. As a secondary backup, another remedy is based on the local monitoring of the voltage control devices. Once the bad data is detected, coordinated control is relinquished and the predetermined set-points are designed based on the worst case scenarios. The approach, proposed here, is validated with a realistic distribution system and is shown to have satisfactory results. The proposed method will assist the DNO/DMS to take immediate and effective VVC decisions when the measurements are tampered with.

REFERENCES

[1] "Uk wants sustained cuts to solar panel tariffs." [Online]. Available: http://uk.reuters.com/article/uk-solar-tariff-idUKTRE8180XS20120209.

[2] V. A. Evangelopoulos, P. S. Georgilakis, and N. D. Hatziargyriou, "Optimal operation of smart distribution networks: A review of models, methods and future research," *Electr. Power Syst. Res.*, vol. 140, pp. 95–106, 2016.

[3] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/var control and countermeasures," in *Proc. 2014 Amer. Control Conf.*, 2014, pp. 4372–4378.

[4] Y. Isozaki *et al.*, "Detection of cyber attacks against voltage control in distribution power grids with PVs," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1824–1835, Jul. 2016.

[5] D. Shelar and S. Amin, "Security assessment of electricity distribution networks under DER node compromises," in *IEEE Trans. Control Netw. Sys.*, vol. 4, no. 1, pp. 23–36, Mar. 2017.

[6] A. P. Kenneth and K. Folly, "Voltage rise issue with high penetration of grid connected PV," *IFAC Proc. Volumes*, vol. 47, no. 3, pp. 4959–4966, 2014.

[7] M. Mahmud, M. Hossain, and H. R. Pota, "Analysis of voltage rise effect on distribution network with distributed generation," *IFAC Proc. Volumes*, vol. 44, no. 1, pp. 14796–14801, 2011.

[8] A. Madureira and J. P. Lopes, "Coordinated voltage support in distribution networks with distributed generation and microgrids," *IET Renewable Power Gener.*, vol. 3, no. 4, pp. 439–454, 2009.

[9] T. S. Basso, IEEE 1547 and 2030 Standards for distributed energy resources interconnection and interoperability with the electricity grid. Nat. Renewable Energy Lab., Golden, CO, USA, Tech. Rep. NREL/TP-5D00-63157, 2014.

[10] A. R. Malekpour and A. Pahwa, "Reactive power and voltage control in distribution systems with photovoltaic generation," in *Proc. North Amer. Power Symp.*, 2012, pp. 1–6.

[11] Z. Shen, "Centralized and Decentralized Volt/Var Control Schemes for the FREEDM System," Ph.D. dissertation, North Carolina State Univ., Raleigh, NC, USA, 2013.

[12] R. Uluski, "Vvc in the smart grid era," in *Proc. IEEE PES Gen. Meeting*, 2010, pp. 1–7.

[13] T. Senjyu, Y. Miyazato, A. Yona, N. Urasaki, and T. Funabashi, "Optimal distribution voltage control and coordination with distributed generation," *IEEE Trans. Power Del.*, vol. 23, no. 2, pp. 1236–1242, Apr. 2008.

[14] S. Paudyal, C. A. Canizares, and K. Bhattacharya, "Optimal operation of distribution feeders in smart grids," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4495–4503, Oct. 2011.

[15] "A review of smart meters rollout for electricity in the energy community." Energy Community regulatory Board, Vienna, Austria, Rep. R10-CWG-13-06, 2010.

[16] Staff, F. E. R. C., "Assessment of demand response and advanced metering." *Federal Energy Regulatory Commission, Docket AD-06-2-000*, 2006.

[17] A. Abur and A. Exposito, *Power System State Estimation, Theory and Implementation*. Boca Raton, FL, USA: CRC Press, 2004.

[18] A. Monticelli, *State Estimation in Electric Power Systems, A Generalized Approach*, (Luwer's power Electronics and power Systems Series). New York, NY, USA: Springer-Verlag, 2004.

[19] J. Chen and A. Abur, "Placement of PMUS to enable bad data detection in state estimation," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1608–1615, Nov. 2006.

[20] A. Majumdar and B. C. Pal, "Bad data detection in the context of leverage point attacks in modern power networks," *IEEE Trans. Smart Grid*, vol. PP, no. 99, p.1, 2017.

[21] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. 1st Workshop Secure Control Syst., Stockholm*, pp. 1–6, 2010.

[22] B. Ramachandran and G. T. Bellarmine, "Improving observability using optimal placement of phasor measurement units," *Int. J. Electr. Power Energy Syst.*, vol. 56, pp. 55–63, 2014.

[23] P. A. Garcia, J. L. R. Pereira, S. Carneiro, V. M. da Costa, and N. Martins, "Three-phase power flow calculations using the current injection method," *IEEE Trans. Power Syst.*, vol. 15, no. 2, pp. 508–514, May 2000.

[24] P. A. N. Garcia, J. L. R. Pereira, and S. Carneiro, "Voltage control devices models for distribution power flow analysis," *IEEE Trans. Power Syst.*, vol. 16, no. 4, pp. 586–594, Nov. 2001.

[25] G. L. Torres and V. H. Quintana, "An interior-point method for nonlinear optimal power flow using voltage rectangular coordinates," *IEEE Trans. Power Syst.*, vol. 13, no. 4, pp. 1211–1218, Nov. 1998.

[26] A. Schellenberg, W. Rosehart, and J. Aguado, "Cumulant-based probabilistic optimal power flow (p-opf) with gaussian and gamma distributions," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 773–781, May 2005.

[27] A. Schellenberg, W. Rosehart, and J. Aguado, "Cumulant based probabilistic optimal power flow (p-opf)," in *Proc. Int. Conf. Probabilistic Methods Appl. Power Syst.*, 2004, pp. 506–511.

[28] P. Zhang and S. T. Lee, "Probabilistic load flow computation using the method of combined cumulants and Gram-Charlier expansion," *IEEE Trans. Power Syst.*, vol. 19, no. 1, pp. 676–682, Feb. 2004.

[29] F. Ruiz-Rodriguez, J. Hernandez, and F. Jurado, "Probabilistic load flow for photovoltaic distributed generation using the Cornish–Fisher expansion," *Electr. Power Syst. Res.*, vol. 89, pp. 129–138, 2012.

[30] Energy Networks Association, "Engineering recommendation G83," *The connection of small-scale embedded generators (up to 16 A per phase) in parallel with public low voltage distribution networks*, no. 2, Aug. 2012.

[31] Energy Network Association, "Engineering recommendation G59," *Recommendations for the Connection of Generating Plant to the Distribution Systems of Licenced Distribution Network Operators*, no. 3, Amendment 1, Aug. 2014.

[32] R. Singh, B. Pal, and R. Jabr, "Distribution system state estimation through gaussian mixture model of the load as pseudo-measurement," *IET Gener., Transmis. Distrib.*, vol. 4, no. 1, pp. 50–59, 2010.

Ankur Majumdar (S'12–M'16) received the B.E.E. (with honours) degree in electrical engineering from Jadavpur University, Calcutta, India, in 2009, the M.Tech. degree in electric power systems from the Indian Institute of Technology, Delhi, India in 2011, and the Ph.D. degree in electrical power engineering from Imperial College London, London, U.K., in June 2016. He is currently a Research Associate in the Department of Electrical and Electronic Engineering, Imperial College London. His research interests include state estimation, smart grid security, and power system analysis.

Yashodhan P. Agalgaonkar (M'14) received the M.Sc. degree in electrical power engineering from the Chalmers University of Technology, Gothenburg, Sweden, in 2006, and the Ph.D. degree in electrical power engineering from Imperial College London, London, U.K., in 2014. He was a Postdoctoral Researcher in Imperial College London until 2014. From 2006 to 2010, he was with Crompton Greaves, India and with Converteam (now GE Energy), Chennai, India and Berlin, Germany, as a Research Engineer. During his tenure at Crompton Greaves and Converteam, he conducted research on diverse areas of power transmission and distribution operation. Since 2015, he has been a Scientist and Engineer in the Energy and Environment Division, Pacific Northwest National Laboratory, Richland, WA, USA.

Bikash C. Pal (M'00–SM'02–F'13) received the B.E.E. (with honours) degree from Jadavpur University, Calcutta, India, the M.E. degree from the Indian Institute of Science, Bangalore, India, and the Ph.D. degree from the Imperial College London, London, U.K, in 1990, 1992, and 1999, respectively, all in electrical engineering. He is currently a Professor in the Department of Electrical and Electronic Engineering, Imperial College London. His current research interests include state estimation, power system dynamics, and flexible ac transmission system controllers. He is the Editor-in-Chief of IEEE TRANSACTIONS ON SUSTAINABLE ENERGY and a Fellow of the IEEE for his contribution to power system stability and control.

Ralph Gottschalg (M'14) has worked for more than 20 years in photovoltaics. He is leading the Applied Photovoltaics research group at CREST, a group of about 20 people focussing on research into photovoltaic performance and system issues. He is the U.K. lead expert to all international standard bodies concerning photovoltaic modules. The metrology team of the research group provides accredited measurements for the U.K. and international industry.