Detection of Cyber Attacks Against Voltage Control in Distribution Power Grids With PVs

Yasunori Isozaki, Shinya Yoshizawa, *Student Member, IEEE*, Yu Fujimoto, Hideaki Ishii, *Senior Member, IEEE*, Isao Ono, Takashi Onoda, and Yasuhiro Hayashi, *Member, IEEE*

***Abstract*—In this paper, we consider the impact of cyber attacks on voltage regulation in distribution systems when a number of photovoltaic (PV) systems are connected. We employ a centralized control scheme that utilizes voltage measurements from sectionizing switches equipped with sensors. It is demonstrated that if measurements are falsified by an attacker, voltage violation can occur in the system. However, by equipping the control with a detection algorithm, we verify that the damage can be limited especially when the number of attacked sensors is small through theoretical analysis and simulation case studies. In addition, studies are made on attacks which attempt to reduce the output power at PV systems equipped with overvoltage protection functions. Further discussion is provided on how to enhance the security level of the proposed algorithm.**

***Index Terms*—Cyber security, distribution grid, photovoltaic power generation, voltage control.**

I. Introduction

CYBER SECURITY has been recognized as one of the critical issues for realizing safe and reliable energy management systems (see [6], [17]). The role that communication networks play in the supervisory control and data acquisition systems has been rapidly growing due to factors such as the introduction of various distributed generation (DG) including photovoltaic (PV) and wind power generation systems in the power grid. More information must be transmitted and processed to improve their interoperability and efficiency for prediction and control of power generation, consumption, and storage [1]. The wide use of communication networks, however, creates vulnerability to malicious cyber attacks, which are especially harmful if any physical damage can be made on power quality and devices.

At the transmission system level, the problem of detecting cyber attacks through the bad data analysis in state estimators has recently gained much attention. Liu *et al.* [11] pointed out that malicious coordinated manipulation in sensor measurement data can result in significant changes in the estimated states, which are stealthy and not detectable via the conventional least squares estimation methods. This result has motivated many researchers in the area of power systems, control, signal processing, and optimization to study more secure schemes based on static as well as dynamic models of the grid (see [2], [12]–[14], [16], [22]). A common theme among these works lies in the development of systems approach toward cyber security in control systems.

By contrast, security issues at the distribution system level have not been much explored and hence are set as the focus of this paper. In [5] and [10], modeling frameworks of cyber security are presented, taking account of both the grid and the communications, but the effects of data manipulation are not addressed. The recent work of [18] studies stealthy data integrity attacks against voltage control and formulates optimization problems for the attacker to maximize the damage though the systems considered are relatively small scale.

In this paper, we consider how attack detection methods can be introduced in the context of voltage regulation in distribution systems. Our emphasis is placed on the consideration of the impacts on the grid brought by connecting DGs in large quantities [21]. In particular, within the feeder lines, the voltage and current distributions become complicated because of reverse power flows, which cause steady state voltage rise. Conventional control techniques will encounter difficulties to cooperate with such situations since they rely on limited measurements obtained at the substations.

Recently, various methods have been proposed to relieve such voltage rise by introducing some level of cooperation among the devices in the system through communication [3], [4], [7], [15], [23]. In general, there are two elements that contribute to these methods. One is enhanced control of voltage regulation devices such as load ratio control transformers (LRTs), step voltage regulators (SVRs), and shunt capacitors. The other is the capability of DGs for reactive power control through their interfacing power electronics equipments.

As an initial attempt for detecting cyber attacks on distribution systems, we construct a simple algorithm and examine

Manuscript received November 21, 2014; revised March 20, 2015; accepted April 19, 2015. Date of publication May 26, 2015; date of current version June 17, 2016. This work was supported by the Japan Science and Technology Agency under the CREST Program. Paper no. TSG-01156-2014.

Y. Isozaki, H. Ishii, and I. Ono are with the Department of Computational Intelligence and Systems Science, Tokyo Institute of Technology, Yokohama 226-8502, Japan (e-mail: isozaki@sc.dis.titech.ac.jp; ishii@dis.titech.ac.jp; isao@dis.titech.ac.jp).

S. Yoshizawa and Y. Hayashi are with the Department of Electrical Engineering and Bioscience, Waseda University, Tokyo 169-8555, Japan (e-mail: shin-yosi@fuji.waseda.jp; hayashi@waseda.jp).

Y. Fujimoto is with the Advanced Collaborative Research Organization for Smart Society, Waseda University, Tokyo 169-8555, Japan (e-mail: y.fujimoto@aoni.waseda.jp).

T. Onoda is with the System Engineering Research Laboratory, Central Research Institute of Electric Power Industry, Tokyo 201-8511, Japan (e-mail: onoda@criepi.denken.or.jp).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2015.2427380

its security level through simulation case studies. Specifically, we consider a distribution system setup consisting of one feeder whose voltage is regulated by the LRT at the substation. The LRT connects the feeder to a higher voltage system and is capable to change its secondary voltage. To accommodate power injections by PVs, the LRT receives voltage measurements from the sectionizing switches equipped with sensors. In our setting, this information is subject to falsification by an attacker, who can then manipulate voltage regulation. Theoretical analysis is carried out on how to effectively attack the system.

Within this framework, we analyze two types of attacks. The first is more serious, where the attacker aims at voltage violation so that voltage values at many nodes go beyond their admissible range without being detected by the controller. While the chance for power devices in the distribution systems to be damaged may be limited, such violations certainly affect the power quality at the consumers side. Through detailed simulations based on a model and data obtained from residential areas in Japan, we exhibit that the proposed algorithm is capable to narrow the range of such attacks and the potential damages especially when the number of attacked sensors is limited.

The second types of attacks concern attempts to reduce the output power of PVs by exploiting their regulation function to avoid overvoltages. This may be less harmful to the grid or the power quality, but can still cause economic impact on the revenue of PV owners. An interesting aspect of such attacks is that the PV owners are influenced, but may not be able to detect them and take countermeasures while the utility side probably has less economic incentive to improve the situation. Overall, if such attacks spread, they can become a factor that discourages the promotion of PVs. We will see that these second types of attacks can be achieved with less effort for the attacker in terms of the number of sensors to be falsified. Discussions are provided on how the proposed algorithm can be enhanced for raising its security level.

This paper is organized as follows. In Section II, we provide an overview on conventional voltage regulation and the specific control method employed in this paper. Section III describes the class of cyber attacks and the detection algorithm studied; we then formulate optimization problems and find their solutions on effective attacks against the proposed algorithm. In Section IV, the distribution system setting used in the simulations is introduced. Results for the cases without and with PVs are presented in Section V. In Section VI, we further consider the risk of output power losses at PVs caused by malicious attacks affecting their overvoltage protection function. Some concluding remarks are given in Section VII. This paper is based on an earlier conference version [9] and includes more details for simulations and discussions; moreover, Sections III-C and VI have been added.

II. Voltage Regulation in Distribution Systems

In this section, we briefly introduce voltage regulation and then the centralized control method employed in this paper.

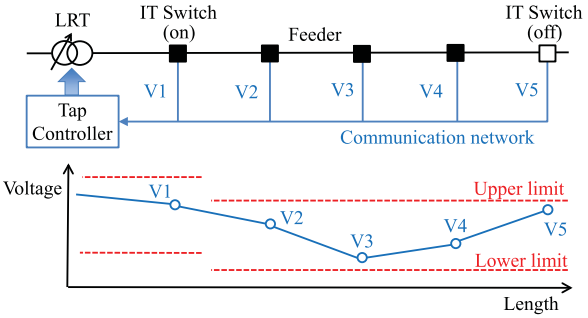


Fig. 1. Voltage regulation via centralized control in a distributed system.

Consider the distribution network model in Fig. 1. Voltage regulation is important for maintaining the quality of power measured by the voltage levels at the consumers side, which must stay within a given admissible range at all times. One of the critical devices used for this control is the LRTs located at distribution substations. These are transformers whose secondary voltage can be varied through switching their taps.

Conventional control is based on the so-called line drop compensator (LDC), which estimates the voltage at a fixed remote point in the network via local measurements at the substation. When there is no injection at any point in the feeder, the voltage profile in the feeder becomes a decreasing function of distance from the substation. Hence, the estimate can be made accurately based on the voltage and the current at the LRT, the topology information, past load data, and so on. However, when DGs are connected, steady state voltage rise may occur within the feeder. This changes the profile characteristics, severely limiting the applicability of LDC.

One solution to this issue is to use sectionizing switches with sensors (called IT switches) in the feeders. Such switches may be equipped with sensors for phase voltages and currents and also have voltage and current transformers. By connecting the switches to the voltage regulator by optical fiber cables, they can send their voltage measurements with sampling periods of, say, 1 min to a half hour. The voltage regulator can then obtain a more accurate voltage profile of the feeder in real time to help determine the necessary output voltage level of the LRT and thus the tap position there.

Notice that the use of voltage measurements in the grid requires real-time data exchange over communication networks. This can raise the risk of cyber attacks, which can harm the performance of voltage regulation. The conventional LDC uses mainly local information and thus may be more robust in this respect; however, as mentioned above, it may fail to regulate properly in the presence of DGs.

Here, we employ a modified version of such centralized control based on those of [7], [23] described as follows. At each sampling time kT, the controller receives the sensor signal $V_i(k)$ of the voltage of each node $i \in \{1, \ldots, N\}$, where T is the sampling period, k is an integer, and N is the number of nodes. The objective is to keep these values within the admissible range as

$$V_{\min,i} \leq V_i(k) \leq V_{\max,i} \text{ for each node } i \tag{1}$$

where $V_{\min,i}$ and $V_{\max,i}$ are, respectively, the lower and upper limit values for the voltage at node i. Let $\Delta V_i(k)$ be the deviation of $V_i(k)$ from the reference $V_{\text{ref},i}$ as

$$\Delta V_i(k) = V_i(k) - V_{\text{ref},i}. \tag{2}$$

Let their minimum and maximum be given, respectively, by

$$\Delta V_{\min}(k) = \min_i \Delta V_i(k), \;\; \Delta V_{\max}(k) = \max_i \Delta V_i(k). \tag{3}$$

Then, the voltage deviation index, which is the sum of these two quantities, is defined by

$$\Delta V_c(k) = \Delta V_{\min}(k) + \Delta V_{\max}(k). \tag{4}$$

The portion of this index $\Delta V_c(k)$ that exceeds the deadzone determined by the constant $\epsilon > 0$ is integrated in time to yield the tap change index $F(k)$ given as

$$F(k) = \sum_{l\in\{0,\ldots,k\}:|\Delta V_c(l)|>\epsilon} T \cdot \text{sgn}(\Delta V_c(l)) \cdot (|\Delta V_c(l)| - \epsilon) \tag{5}$$

where $\text{sgn}(x)$ gives the sign of a scalar x and the deadzone parameter is given by $\epsilon = 90$ V. This index $F(k)$ represents the time integral of voltage violation.

The tap position $\text{Tap}(k)$ is switched when the index $F(k)$ becomes sufficiently large that it exceeds the threshold F_{ref} as

$$\text{Tap}(k+1) = \begin{cases} \text{Tap}(k) + 1 & \text{if } F < -F_{\text{ref}} \\ \text{Tap}(k) - 1 & \text{if } F > F_{\text{ref}} \\ \text{Tap}(k) & \text{otherwise.} \end{cases} \tag{6}$$

We have set the threshold as $F_{\text{ref}} = 15\ \text{V}\cdot\text{s}$ by examining different cases in simulation. Note that the parameters ϵ and F_{ref} have effects on the sensitivity of tap switchings. When they take smaller values, the tap will switch more frequently, reducing the chance of voltage violation, but at the same time increasing the wear in the devices.

III. Cyber Attacks Toward Voltage Violation

The centralized control introduced above requires real-time data communication of the measurements from the switches. This increases the chances of data falsification by malicious attackers, which can result in undesirable changes in the voltage levels in the grid. As discussed in the Introduction, there are two types of potential attacks depending on the kinds of target damages as follows: 1) voltage violation in the feeder; and 2) output power loss at PV systems. To keep the presentation simple, we will begin with the treatment of the first type. In this section, we discuss some attack scenarios of this type and then introduce an algorithm to detect such attacks. Then, we analyze how an attacker can efficiently achieve voltage violation without being detected.

A. Attack Scenarios

In voltage regulation, an attacker may falsify a limited number of sensor measurement data from nodes to manipulate and cause irregular tap changes. This can result in voltage violation at feeder nodes or unnecessary tap changes, which are undesirable because they can cause damages in the devices. Here, we set the objective of the attacker to cause overvoltage and undervoltage as much as possible. It is assumed that the attacker has knowledge on the centralized control method.

There are two approaches to achieve the goal as follows.

1) To suppress tap changes at the LRT to cause:
   a) undervoltage when loads at some nodes increase;
   b) overvoltage when loads at some nodes decrease.
2) To induce tap changes at the LRT to cause:
   a) undervoltage at some nodes by tap switching downward;
   b) overvoltage at some nodes by tap switching upward.

It is useful to denote by $V_i^*(k)$ and by $V_i(k)$, respectively, the true voltage at node i and its sensor measurement received at the LRT at time k. Moreover, the number of attacked nodes is denoted by M. Then, the attackers' objective can be expressed as achieving voltage violation so that for some nodes i and times k, $V_i^*(k) < V_{\min,i}$ or $V_{\max,i} < V_i^*(k)$ subject to remaining undetected by the algorithm to be proposed below and manipulating up to M sensor data as $V_i(k) \neq V_i^*(k)$.

Clearly, if the attacker is able to modify measurements from all sensors, i.e., $M = N$, then it is straightforward to accomplish any of these scenarios. The tap level will be unchanged if, for example, all measurement values from sensors remain at the center of the admissible range. Then, on the other hand, forced tap changes can occur if all sensor values appear together near the upper or lower limit. Though such attacks may be effective in increasing voltage violation, the behavior in sensor values would be irregular. Thus the attacks may be detectable through different measures based on past data on voltage control and conditions of the feeders. Hence, in this paper, we do not deal with the case when all sensors are attacked.

B. Algorithm for Detection of Measurement Falsification

For detection of attacks on the control system, we propose an algorithm to be executed by the voltage regulator at each sampling instant kT. The algorithm checks the sensor measurements and determines whether the current values are normal or not. It consists of four steps as outlined below.

Step 1 (Voltage Measurement Values): Find whether the measurement value V_i of the voltage at each node i falls within the admissible range given in (1).

Step 2 (Order Among Voltage Values): If no power injection is made through PVs at any of the nodes in the system, then check whether for each node, its voltage value is smaller than those upstream (i.e., closer to the LRT). This step may be skipped during the day when PVs are in operation.

Step 3 (Voltage Change Rates): If a tap change did not occur in the previous time step $(k-1)T$, then check whether

$$\left|V_i(k) - V_i(k-1)\right| \leq C(k) \tag{7}$$

where $C(k)$ represents the upper bound; this bound may be found from past data and may vary according to the levels of load and PV generation.

Step 4 (Lower Bound on Voltage Differences): Check whether the following inequality holds:

$$\max_i V_i(k) - \min_i V_i(k) \geq D(k) \tag{8}$$

where $D(k)$ is a given (time-varying) lower bound.

We have some comments on this detection algorithm. Step 1 verifies if any voltage violation has happened in the grid; under any circumstances, such an event should be alarmed. For step 2, the interpretation is as follows: When no PV is present in the grid, the current flows in the downstream direction along the feeder. Hence, at each node, the voltage is lower than those at the nodes upstream. Step 3 is based on the observation that the voltage values change only at a certain rate in general when no tap change took place in the previous control time. Step 4 focuses on the range in the differences among the voltage values; it is useful for detecting manipulations which make all measurement values close to each other.

The detection algorithm above is indeed very simple, being based only on the current and previous voltage values of the nodes. In the following sections, we examine the level of security that this approach can provide and its usefulness in detecting unusual behaviors in the feeder voltage, which may be a result of manipulation by attackers.

C. Analysis on Attack Approaches

So far, we have introduced the possible attack scenarios and then the simple detection algorithm. Here, we analyze how the attacks can be made most effectively to create changes in the control actions without being detected by the algorithm.

The goal of the attacker is to manipulate the tap position in the centralized control so that the voltage is too high/low for the distribution system at the time. Since the tap position is determined by the control law (6), it is clear that, depending on the scenario, the attacker should try to affect the control variables and, in particular, to maximize or minimize the value of $F(k)$ and hence $\Delta V_c(k)$ in the most efficient way at appropriate moments. Based on this observation, the four scenarios 1)a), 1)b), 2)a), and 2)b) of attacks described in Section III-A can be classified into two cases. For each case, we formulate an optimization problem in a slightly simplified setting and show that explicit solutions can be found. The results will become the basis for the simulation case studies in later sections.

Here, to simplify the analysis, we introduce the following assumptions.

1) The feeder has a line topology (i.e., there is no branching) and the nodes are labeled in an ascending order starting from the substation (as in Fig. 1).
2) There is no PV in the system.
3) The number M of nodes attacked satisfies $M \leq N-2$. In particular, node 1 cannot be attacked since it is the closest to the substation and its voltage V_1 can be easily estimated.
4) We ignore steps 3 and 4 in the algorithm.
5) The admissible ranges $[V_{\min,i}, V_{\max,i}]$ for all nodes except node 1 are the same, and $V_{\min,1} > V_{\min,i}$ and $V_{\max,1} > V_{\max,i}$ for $i \neq 1$, i.e., node 1 has a range at higher values.

Note that because of 1) and 2) above, the actual voltage values $V_i^*(k)$ always satisfy the order

$$V_1^*(k) \geq V_2^*(k) \geq \cdots \geq V_N^*(k). \tag{9}$$

We can relax assumption 1) on the feeder structure from line topologies to tree topologies. However, results at that generality will require further analysis. Also, under this setting, we obtain sufficient intuition about attacks for the case studies carried out later. Regarding assumption 4), our analysis here is a static one, and hence the attacker should aim at reaching the solutions outlined below by slowly changing measurements to avoid violating step 4 in the detection algorithm; moreover, step 3 is easy to take into account in the attacks if necessary.

1) Maximization of $\Delta V_c(k)$: In scenario 1)a), the attacker tries to suppress the tap from switching upward when the load level goes up, which can result in undervoltage at some nodes. This means that $\Delta V_c(k)$ should be made larger than its actual value, which is denoted by $\Delta V_c^*(k)$. In particular, it is necessary to attain

$$\Delta V_c(k) \geq -\epsilon \text{ when } \Delta V_c^*(k) < -\epsilon. \tag{10}$$

This condition may need to be maintained for a certain period of time since $F(k)$ involves the time integral of $\Delta V_c(k)$. Similarly, in scenario 2)a), the aim is to induce tap change downward so that undervoltage may occur; it is clear that such attacks require the maximization of $\Delta V_c(k)$ as well.

The attacker can falsify up to M measurements. Hence, the most efficient way of attack will be based on the following maximization problem:

$$\begin{aligned} \text{Maximize} \quad & \Delta V_c(k) \\ \text{subject to} \quad & V_{\min,i} \leq V_i(k) \leq V_{\max,i} \text{ for } i \\ & V_1(k) \geq \cdots \geq V_N(k) \\ & \left|\left\{i : V_i(k) \neq V_i^*(k)\right\}\right| \leq M \\ & V_1(k) = V_1^*(k) \end{aligned} \tag{11}$$

where $|\cdot|$ is the cardinality of a set. In this problem, by the first and second constraints, the attacks will be consistent with steps 1 and 2 in the detection algorithm and hence will not be detected. The third constraint shows that the number of attacked nodes is less than or equal to M. The fourth one comes from assumption 3) on node 1.

The solution to this problem can be derived explicitly and is given by

$$V_i(k) = \begin{cases} \min\left\{V_1^*(k), V_{\max,2}\right\} & \text{if } i = 2 \\ V_{N-M+1}^*(k) & \text{if } i = N-M+2, \ldots, N \\ V_i^*(k) & \text{otherwise.} \end{cases} \tag{12}$$

This can be established as follows. By (4), we have $\Delta V_c(k) = \Delta V_{\min}(k) + \Delta V_{\max}(k)$. It is thus enough to separately maximize $\Delta V_{\min}(k)$ and $\Delta V_{\max}(k)$ as long as the constraint on M is satisfied. First, to maximize $\Delta V_{\max}(k)$, it is sufficient to modify $V_2(k)$ whose value must be the largest according to the order among $V_i(k)$, but should also be within the admissible range. Thus, $V_2(k)$ must be no larger than both $V_1^*(k)$ and $V_{\max,2}$. [Because of assumption (5), $V_1^*(k)$ can be

larger than $V_{\max,2}$.] Then, from (3), we obtain the maximum of $\Delta V_{\max}(k)$ as

$$\begin{aligned}\max \Delta V_{\max}(k) &= \max V_2(k) - V_{\mathrm{ref},2} \\ &= \min\left\{V_1^*(k), V_{\max,2}\right\} - V_{\mathrm{ref},2}. \end{aligned} \quad (13)$$

On the other hand, by modifying the remaining $M-1$ measurements, the value $\Delta V_{\min}(k)$ can be maximized without violating the order constraint. As a result, we have

$$\max \Delta V_{\min}(k) = V_{N-M+1}^*(k) - V_{\mathrm{ref},N-M+1}. \quad (14)$$

Thus, from (13) and (14), the maximum value of $\Delta V_c(k)$ can be found as

$$\begin{aligned}\max \Delta V_c(k) &= \max \Delta V_{\min}(k) + \max \Delta V_{\max}(k) \\ &= V_{N-M+1}^*(k) - V_{\mathrm{ref},N-M+1} \\ &\quad + \min\left\{V_1^*(k), V_{\max,2}\right\} - V_{\mathrm{ref},2}. \end{aligned} \quad (15)$$

It is clear that attacks based on the above solution may or may not result in undervoltage. The level of undervoltage will depend on various factors such as the number M of attacks, the load level, the tap position at the time, and so on. For example, in scenario 1)a), the damage will be large especially if the attack is made at the time when loads in the distribution system becomes high and consequently, the voltage in the feeder becomes low.

One aspect not considered in the above formulation is the possibility of detection after the occurrence of undervoltage. Obviously, if the number of nodes whose voltage $V_i^*(k)$ go under their lower limits is greater than $M-1$, then the algorithm will detect by step 1 because for such nodes, their values satisfy $V_i(k) = V_i^*(k) < V_{\min,i}$. In the case study simulations, we will examine these issues in detail.

As discussed above, attacks need to affect $F(k)$, which involves the time integral of $\Delta V_c(k)$. Hence, in general, the attacks need to be persistent in time. This fact may rule out the effectiveness of more bursty types of attacks.

2) Minimization of $\Delta V_c(k)$: A similar analysis can be made for the scenarios 1)b) and 2)b), where in these cases, the problem becomes that of minimization

$$\begin{aligned}&\text{Minimize} \quad \Delta V_c(k) \\ &\text{subject to (11).}\end{aligned} \quad (16)$$

The solution can be obtained as

$$V_i(k) = \begin{cases} V_{M+1}^*(k) & \text{if } i = 2, \ldots, M \\ V_{\min,N} & \text{if } i = N \\ V_i^*(k) & \text{otherwise} \end{cases} \quad (17)$$

and the optimal value of $\Delta V_c(k)$ is expressed as

$$\min \Delta V_c(k) = V_{\min,N}(k) - V_{\mathrm{ref},N} + V_{M+1}^*(k) - V_{\mathrm{ref},M+1}. \quad (18)$$

This problem is in fact easier than the maximization counterpart because for node N, in order to minimize $\Delta V_{\min}(k)$, it is always best to modify $V_N(k)$ to the smallest value $V_{\min,N}$ in the admissible range, and there is no issue like node 1 whose value cannot be attacked.

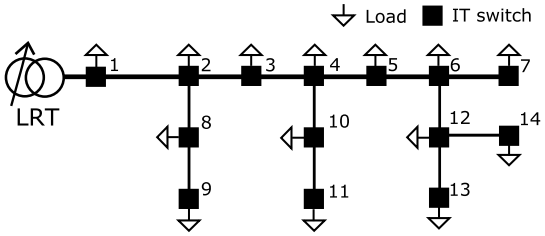


Fig. 2. 6.6-kV network in the distribution system model.

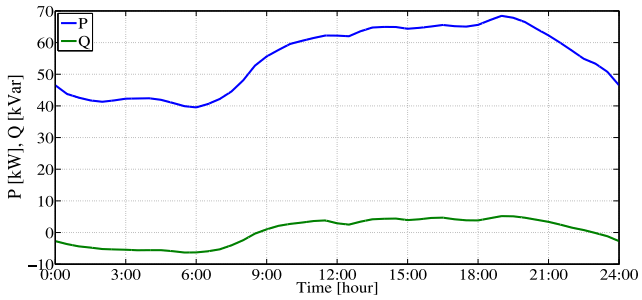


Fig. 3. Profile of high-voltage loads at nodes 3, 5, 8, 9, 11, 12, and 13.

IV. Simulation Settings

In this section, we describe the setup for simulations that we performed for verifying the detection algorithm.

A. Network Model

For our simulation studies, we employed a distribution network in a residential area with one feeder. It has been set up under the project of [8] as a testbed system to be shared for the purpose of verifying various novel energy management techniques. The network models a small size residential district in Japan and uses parameters and load profiles based on real data. In Fig. 2, the 6.6-kV network with 14 nodes is shown. Voltage regulation is carried out by the LRT, connected to a steady voltage source of 66 kV. Its tap width is set as 30 V.

Each node in the figure represents a sectionizing switch together with a pole transformer, which is connected to a low-voltage 100 V network. In total, there are 435 residents in the low-voltage networks. Moreover, high voltage loads are directly connected at nodes 3, 5, 8, 9, 11, 12, and 13. The total contract demand in the system is set as 2113 kVA.

For the low-voltage network in Japan, the secondary voltage at pole transformers is regulated within the admissible range [103, 107] V. By converting this range to the 6.6-kV system side, the reference values have been chosen as $V_{\mathrm{ref},1} = 6750$ V for node 1 and $V_{\mathrm{ref},i} = 6600$ V for $i = 2, \ldots, 14$. Also, we set the admissible range in (1) as $[V_{\min,1}, V_{\max,1}] = [6621, 6879]$ V for node 1 and $[V_{\min,i}, V_{\max,i}] = [6474, 6726]$ V for other nodes $i = 2, \ldots, 14$. Note that node 1 is given a different reference since the line between nodes 1 and 2 is long.

In the simulations, for all loads, profiles obtained from a Japanese power company were used with minor modifications. For the high-voltage loads, a common profile as shown in Fig. 3 was employed, which also contains reactive power.

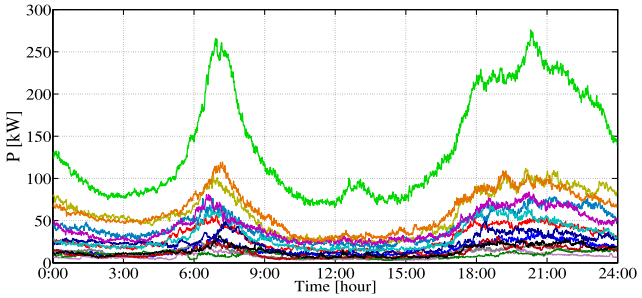


Fig. 4. Profile of aggregated low-voltage loads at all nodes.

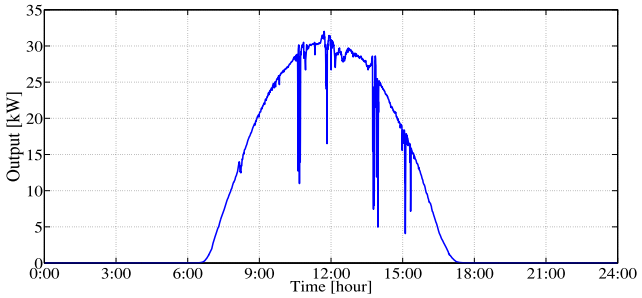


Fig. 5. Example of PV generation profile.

For the low-voltage ones, aggregated profiles at the pole transformers were generated, as shown in Fig. 4.

In this model, we assume that each residence is equipped with a PV system. The PV generation profiles are also based on real data. Moreover, the residences are assumed to be located near to each other and thus have similar weather and solar radiation conditions. As a consequence, the generated power is roughly synchronized among the PVs, for example, when clouds come to the area causing sudden drops in PV generation. From the viewpoint of voltage regulation, this is in fact a harsher condition compared to situations when the PVs are more spread out in a wider area. In such cases, PV generation profiles would differ more among residences and hence spikes in individual profiles will be smoothened when a large number of them are aggregated.

For the simulation, we employed real PV profile data collected on a sunny day with some clouds at different locations in a Japanese city. One instance of the data is depicted in Fig. 5. It is noted that we have conducted case studies based on other PV generation conditions such as cloudy days and partially cloudy days; it was found that the qualitative nature of the results were similar to what is reported in this paper.

B. Voltage Control Under Normal Conditions

The centralized control introduced earlier has been applied to this network setting for two cases: 1) without PVs; and 2) with PVs.

1) For the case when all PVs are turned off, the time responses of the voltage values $V_i(k)$ over 24 h at the 14 nodes are depicted in Fig. 6; the line colors for node voltages used in the plots are shown in Fig. 8, which will be used consistently throughout this paper. The (blue) line appearing on the top represents the voltage at node 1, whose reference value is larger than others; it is almost piecewise constant and in fact closely follows the tap changes, which occurred approximately at hours 7:00, 17:00, 18:30, and 23:00. The dashed lines indicate the upper and lower limits of the admissible range for other nodes. We confirm that the control accomplishes to keep all node voltage in this range.

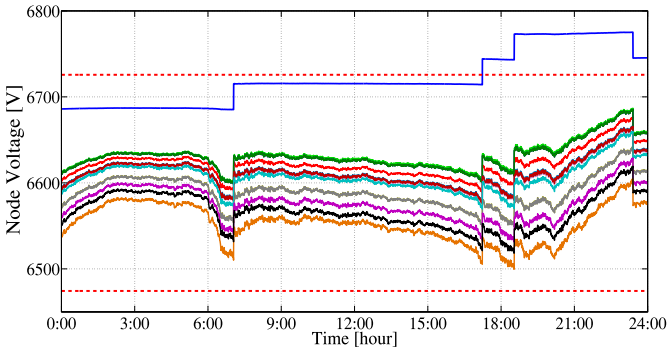


Fig. 6. Normal case without PVs: voltage time responses.

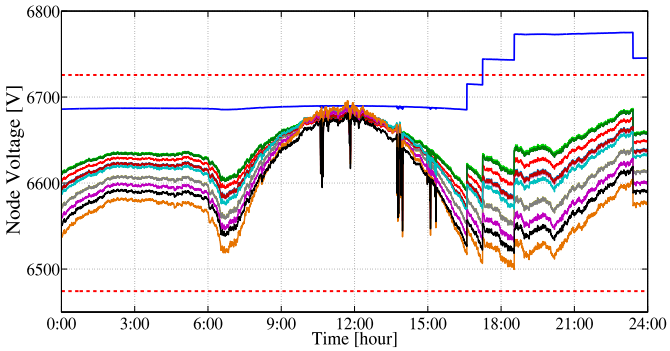


Fig. 7. Normal case with PVs: voltage time responses.

Fig. 8. Line colors of the 14 nodes used in the figures.

2) For the case with PV generation, a similar plot of the node voltage is given in Fig. 7. Notice that during the day, the voltage values become very close due to reverse power flows resulting from PVs. In fact, at these hours, the voltage values do not follow the order in step 2 of the detection algorithm, which is hence not applicable. Different from the case without PVs, no tap change occurred in the morning because the power generated by PVs is consumed during the day time. However, note that to provide sufficient power through the LRT in the evening, there are four tap changes starting in late afternoon, roughly at 16:30, 17:15, 18:30, and 23:30.

C. Parameters for the Detection Algorithm

For the network topology of Fig. 2, the order among voltage values in step 2 in the detection algorithm of Section III-B

becomes as follows:

$$\begin{aligned}
&\text{(i)} \quad V_1(k) > V_2(k) > V_3(k) > V_4(k) \\
&\qquad\qquad > V_5(k) > V_6(k) > V_7(k) \\
&\text{(ii)} \quad V_2(k) > V_8(k) > V_9(k) \\
&\text{(iii)} \quad V_4(k) > V_{10}(k) > V_{11}(k) \\
&\text{(iv)} \quad V_6(k) > V_{12}(k) > V_{13}(k) \\
&\text{(v)} \quad V_{12}(k) > V_{14}(k). \qquad (19)
\end{aligned}$$

In general, the order among the voltage values at the end nodes, that is, nodes 7, 9, 11, 13, and 14, is not known *a priori*.

For steps 3 and 4, the bounds $C(k)$ and $D(k)$ were chosen based on the simulation results under normal conditions: $C(k) = 0.02$ V and $D(k) = 40$ V if no PV is in operation, and $C(k) = 4.0$ V and $D(k) = 10$ V, otherwise.

V. Simulation Results

For the simulations under cyber attacks, we mainly concentrated on scenario 1)a) among those outlined in Section III-A; we will later discuss the potentials of other scenarios. In this scenario, the attacker aims at keeping the tap of the LRT from switching upward. In each of the cases without and with PVs in Figs. 6 and 7, we notice that three out of four tap switches were upward. Different attacks can be generated depending on the disabled tap changes.

For the attacks, we follow the approach discussed in Section III-C. Given the number M of nodes to be attacked, we generate measurement falsifications based on the analytical solution (12) (with slight modifications) to maximize the parameter $\Delta V_c(k)$ in the centralized controller as follows.

1) To falsify the sensor data $V_2(k)$ from node 2 to be as large as possible, that is

$$V_2(k) = \min\left\{V_1^*(k),\ V_{\max,2}\right\}. \qquad (20)$$

2) To increase the $M-1$ measurements $V_i(k)$ for the nodes taking low voltage values. The falsified value of any node should remain smaller than those of nodes in upstream to respect the voltage order in (19) during the hours when no PV generates.

We will confirm that these attacks can disable the LRT to change its tap upward for increasing its voltage output. At the same time, the algorithm in Section III-B cannot detect them. In particular, steps 1 and 2 will not be violated. As we will see in the simulations, it is important to falsify $V_i(k)$ of nodes whose true voltages violate the lower limit as $V_i^*(k) < V_{\min,i}$ when the load in the system goes up. This is necessary for any undervoltage not to be detected via step 1 in the detection algorithm.

Node 1 is assumed to be secure since its voltage can be estimated at the substation through its secondary voltage and current, and line properties. Through simulations, we studied the relation between the number M of falsified sensors and the resulting damage. We first describe the simpler case without PVs and then explain the differences in the case with PVs.

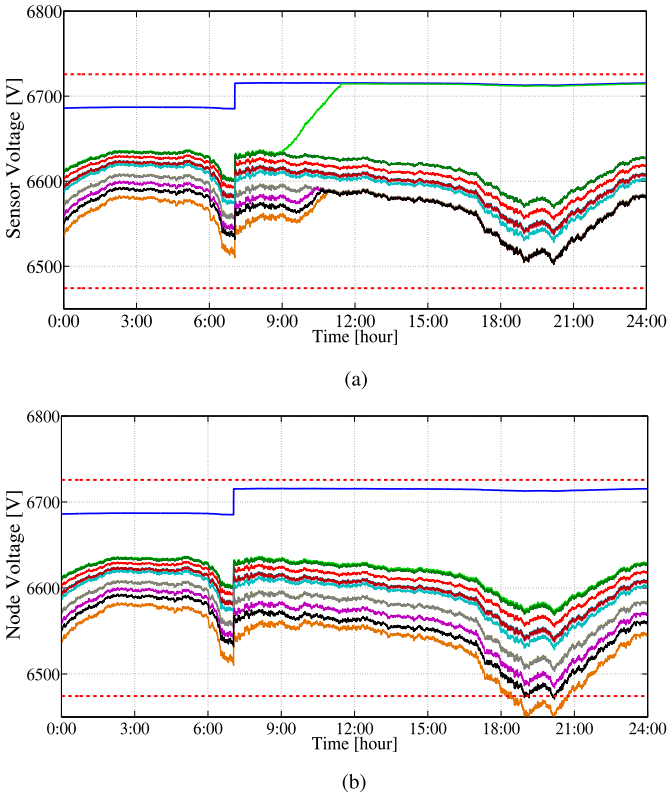


Fig. 9. Without PV power generation: attacks on five nodes. Time responses of (a) sensor measurements and (b) voltage values.

A. Case I: Without PV Power Generation

For this case, it was found that the level of damage could be classified into three cases based on the number M of falsified sensors. Each case is described in the following.

First, when only one or two sensors are attacked ($M = 1, 2$), the detection algorithm was always able to find the attacks. Under the attack scenario here, one of the attacks is always targeted at node 2 based on (20); its modified sensor value satisfies the constraints in steps 2 and 3 of the algorithm and hence the attack cannot be detected from the behavior of this node. As we will see more in detail next, the attacks create undervoltage in the system, but always at two or more nodes. This means that at least one node whose sensor is not falsified will have its voltage go below the lower limit; at that point, step 1 in the algorithm will alarm. Of course, the maximum number of attacked nodes for the algorithm to detect depends on the feeder topology as well as on other factors.

Next, when the number of attacked sensors is raised to $M = 3, 4, 5$, undervoltage could be made at nodes 13 and 14. The responses of the measurements are given in Fig. 9(a) and those of the actual node voltages in Fig. 9(b). Here, the attacker slowly increased the sensor value $V_2(k)$ of node 2 after 8:00 until it reached $V_1^*(k)$. This in turn made it possible to prevent two upward changes in the tap at 17:00 and 18:30 in Fig. 6. Then, the two nodes of 13 and 14 experienced voltage violation. As long as the sensor measurements at these nodes are falsified so as to keep them above the lower limit, the attack will not be detected by the algorithm. In Fig. 9(a),

TABLE I
VOLTAGE VIOLATION CAUSED BY ATTACKS (IN V · S)

M: # of attacked nodes	Without PVs	With PVs
1–2	0	0
3–5	1.00×10^5	1.00×10^5
6–12	7.86×10^5	7.85×10^5

the attacks on these nodes were made after 11:00 as

$$V_7(k) = V_{12}(k) = V_{13}(k) = V_{14}(k) = V_6^*(k). \tag{21}$$

The last case is when the attack (20) at node 2 started at an earlier time of 0:00. Then, all tap changes could be disabled, resulting in a larger amount of undervoltage. This attack requires six or more measurements to be falsified ($M \geq 6$). Here, for nodes 6, 7, 12, 13, and 14, voltage went below the lower limit after 17:00. This is the time when power consumption at residences increases in the evening, which can be understood from the load profile of Fig. 4. For the voltage violation to be unnoticed by the detection algorithm, as in (21), we set $V_6(k) = V_7(k) = V_{12}(k) = V_{13}(k) = V_{14}(k) = V_5^*(k)$.

To compare the three cases, the damage due to the attacks in terms of the amount of voltage violation is summarized in Table I, where the unit is V·s. It is obvious that, as expected, the larger the number M of attacked nodes, the damage becomes more. However, another feature, which may be less intuitive, is that the amount of damage changes only in a discrete manner and is not a strictly increasing function of M. The reason is that physical damage in voltage quality results only through changing the tap behavior at the LRT. In the current scenario 1)a), tap changes that would take place under the normal condition are prevented by the attacks and hence only a limited number of attack patterns exists.

B. Case II: With PV Power Generation

By applying similar techniques for the attacks, we simulated the case when the PVs connected to the low-voltage networks are turned on. As mentioned in Section III-B, the detection algorithm is less capable since, for example, step 2 (for checking the order among sensor values) is not applicable. This seems to indicate that the voltage control system is more vulnerable to the considered class of attacks.

However, this is true only to a certain extent. In fact, the range of attacks as well as the damage in voltage violation are not much different from the previous case as can be seen in Table I. Notice that the responses under normal conditions in Fig. 7, all tap changes take place in the early evening. By this hour, the voltage values at the nodes become similar to those in the case without PVs, and hence disabling the tap changes results in undervoltage at a similar level.

The attacks required to achieve these results are somewhat more complicated. To give an example, we exhibit the case when three to five nodes are attacked in Fig. 10(a) and (b) for the responses of the sensor values and the true voltages, respectively. Here, the upward tap change at 18:30 in the normal case is being canceled [scenario 1)a)] while an unnecessary tap change downward takes place around 17:00 [scenario 2)a)]. To achieve this, in Fig. 10(a), the sensor value V_{13} of node 13 starts decreasing around 13:00, but then increases after 16:00 together with node 2 whose measurement starts tracking that of node 1. In Fig. 10(a), we observe undervoltage at nodes 13 and 14.

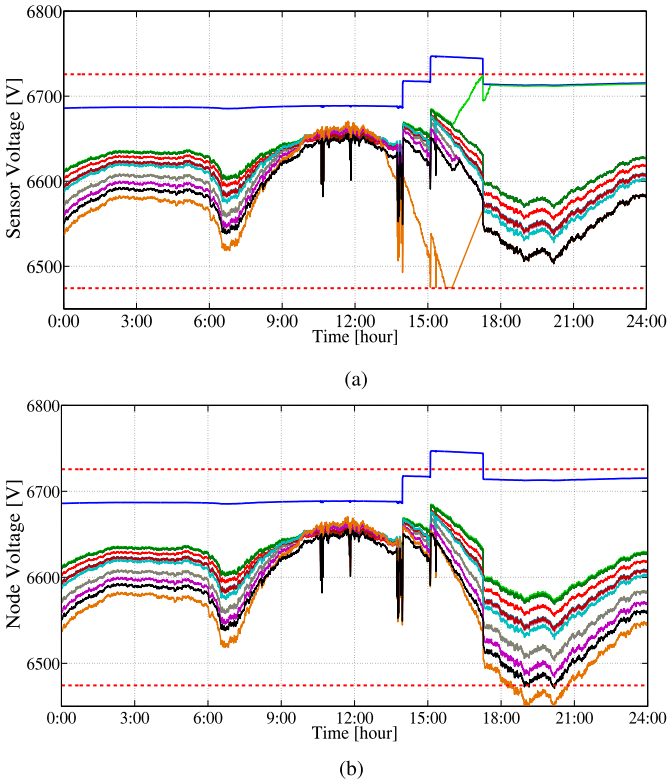


Fig. 10. With PV power generation: attacks on five nodes. Time responses of (a) sensor measurements and (b) voltage values.

C. Discussion

We have demonstrated above that the proposed simple algorithm can detect attacks when the number of sensor values modified is small ($M = 1$ or 2) and moreover the level of damage is limited even if the number is larger ($M = 3, 4$, or 5). Note that in our studies, we have assumed that all switches have voltage sensors, but if some of them do not, then estimation will be necessary for such switches; this can create more vulnerability to the overall system.

There are several ways to further enhance the security level. One is to more carefully watch the voltage of node 2. In all cases, it was necessary to increase its value to that of node 1; without doing so, the tap change (upward) will not be disabled. However, this is unnatural since according to the setting, the line between these nodes is long and hence sufficient difference is expected. It should be noted that keeping the value of node 2 smaller than that of node 1 will reduce the impact of the attack, as tap changes cannot be fully disabled and occur at later times than in the normal case. Another (obvious) solution for better protection is to make node 2 more secure by other means to reduce the chance to be falsified. When severe attacks are detected, the system operator should consider measures such as changing the communication protocol

or switching the controller to the conventional LDC, which does not use any communication.

So far, we considered the attack scenario 1)a) among those described in Section III-A, but other ones are possible as well. Scenario 1)b) requires a pattern opposite to 1)a) in the sense that overvoltage should occur when the loads decrease late at night; this can be achieved by generating extra tap changes upward in the evening and then keeping the high voltage by suppressing tap changes at night. We confirmed via simulation that such attacks are possible.

On the other hand, it seems more difficult for attacks of scenarios 2)a) and b) to result in voltage violation without being detected. For this approach to be successful, it is necessary to generate forceful tap changes sufficiently many times for some nodes to violate the admissible range. One exception is the case when all 13 nodes are falsified. (Note that we have assumed that node 1 is secure.) This is of course the most severe case in terms of potential damages on the system. A variety of malicious attacks can be made though they tend to be somewhat trivial, e.g., to keep all sensor measurements close to the lower/upper limit.

VI. Attacks Toward PV Output Power Loss

In this section, we consider the distribution network where the PV systems are equipped with output regulation functions. In this case, another attack scenario is possible, targeting losses in PV output power. This type of attack may be less harmful to the distribution system, but would be problematic for PV owners and also from the viewpoint of efficient use of PV generated power. We first describe the output regulation function and then present simulation results. It is shown that harmful attacks can be generated relatively easily, which may be difficult to detect by the proposed algorithm.

A. PV Systems With Overvoltage Protection Functions

As we have seen in the previous section, power injection from PV systems can raise the voltage in the distribution line. To locally provide overvoltage protection, PV systems are usually equipped with power conditioning systems (PCS) to regulate their outputs [20]. This can be realized through active and/or reactive power control. The PCS starts to control the PV output when its voltage exceeds a certain starting threshold and then stops the control when the voltage becomes lower than a recovery threshold. Typically, the recovery threshold is set to be lower than the starting threshold so as to avoid unnecessary fast oscillations in the output. Controlling active power is known to be more effective in reducing the voltage level and is hence more common in PCSs.

Ueda *et al.* [20] described how some residences may experience more output power loss depending on, e.g., their locations within the feeder and the threshold parameters used in their PCSs, based on test case data. In [19], it is demonstrated that in fact, those parameters can be determined in a systematic manner to reduce the imbalance in the output power losses among residences.

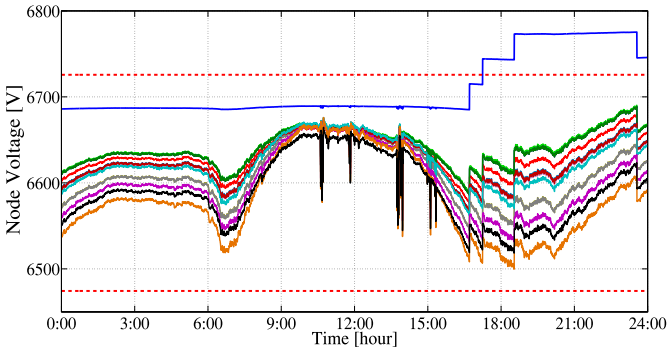


Fig. 11. Normal case with PV output regulation: voltage time responses.

B. Simulation Results

We continue with the case from the previous section where PV systems are installed in each residence. Here, we further assumed that the PVs are equipped with the same PCS that enforces only active power control. The starting threshold is 106.5 V and the recovery one is 106.0 V. Once the control starts, it reduces the output at the fixed rate of 2%/s and as it recovers the output, the rate will be at 4%/s.

We first ran the simulation in the normal condition when such PCSs are present in operation under the same setting as that when PVs are connected in Fig. 7. In Fig. 11, the responses of the voltage values are shown. In comparison, the suppression of the voltage rise during the day is noticeable since the voltage level do not change much between 10:00 and 14:00. The profiles, however, look similar during the night and early morning when no PV output is generated.

Malicious attacks can easily create output power losses by affecting the tap control. In particular, we follow attack scenario 2)b) to raise the overall voltage level in the system by forced tap changes so that the PCSs will turn on. The case considered is with one sensor falsification, i.e., $M = 1$. By the attack solution in (17) for scenario 2)b), the sensor value of node 13 at the end of the feeder taking the lowest voltage value is modified to slowly achieve $V_{13}(k) = V_{\min,13}$.

The results are shown in Fig. 12 where we see forced upward tap changes in early morning around 6:00. If the protection function of the PCSs does not take part and the tap remains at the same position, then overvoltage would occur at all nodes in the day time; this attack will be detected by the proposed algorithm unless all sensor values are falsified. In the current simulation setting, such overvoltage is avoided by the protection function of PCSs. We observe that the voltage levels at all nodes do not change much between 8:00 and 16:00.

We measure the damage caused by these attacks through the output losses of the PV systems. Fig. 13 summarizes the power output of the PVs in one day at each residence located under different nodes for the following three cases: 1) when no PCS is used (Fig. 7); 2) when PCSs are in operation (Fig. 11); and 3) when the attacks explained above affected the PCSs (Fig. 12). We see that for the case without PCS, the power level generated at different nodes vary, but are quite similar. Once the PCSs are introduced, output

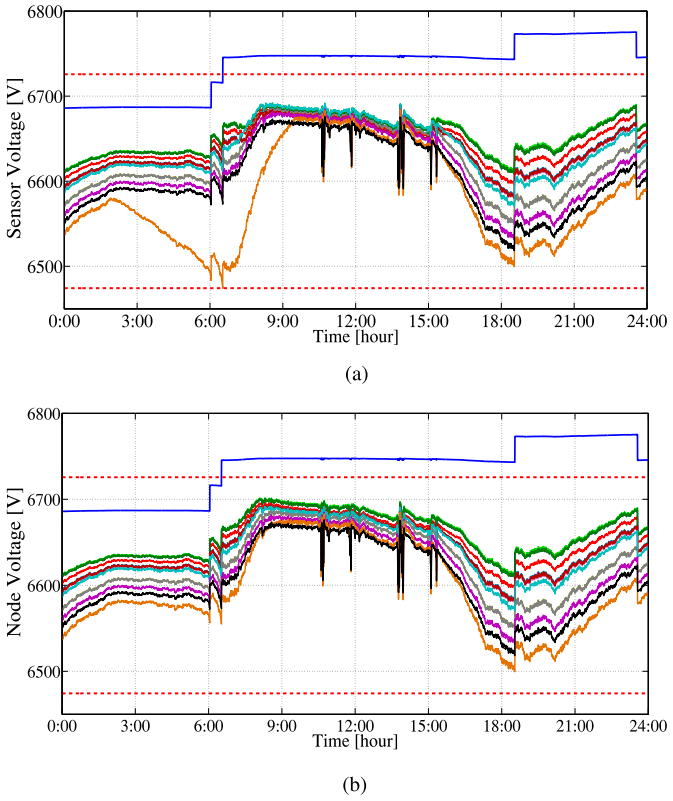


Fig. 12. With PV output regulation: attacks on one node. Time responses of (a) sensor measurements and (b) voltage values.

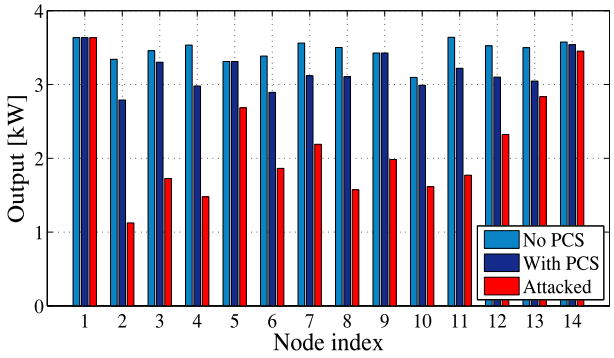


Fig. 13. PV output power determined by PCSs.

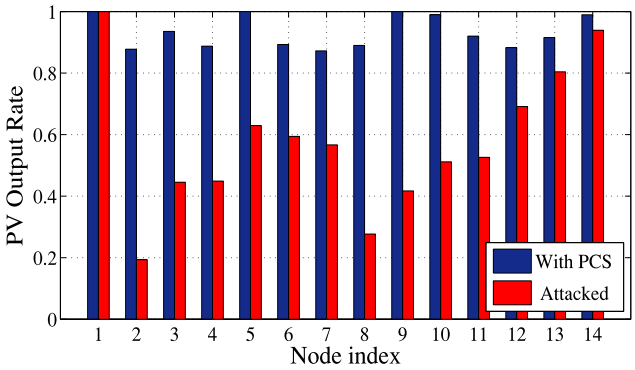


Fig. 14. Rate of PV output power determined by PCSs.

losses do occur. However, it is evident that the attacks can cause additional losses, which can be significant especially at, e.g., nodes 2, 8, and 9.

To show the amount of losses more clearly, we plot in Fig. 14 the rates in the PV outputs for the cases 2) and 3) with respect to 1). That is, the output at each residence without PCS is set to be 1 and then the ratios in outputs with PCSs are plotted for the normal and attacked cases. In the normal case, nodes experience output power losses of less than 15% while in the attacked case, output losses can be as large as 80% (at node 2). It is interesting to note that nodes more in the upstream experience higher losses; the reason is that at such nodes, the original voltage is higher.

C. Discussion

We have shown above that in addition to attacks resulting in voltage violation in the feeder, it is possible to induce unnecessary regulation of the PV output power, which can create economic losses for PV owners.

Such attacks are less harmful from the viewpoint of the distribution systems: Different from the attacks in the previous section, none of the devices in the distribution system will experience dangerous conditions. Since the responsibility of the level of power generation by PV systems rests on the owners, it is unlikely that the considered attacks will be detected at the distribution system level. However, the attacks will be problematic for PV owners expecting to raise certain revenue by selling redundant power. Furthermore, they would result in damaging the effective use of DGs and may require additional costs to monitor for prevention. An obvious solution for PV owners is to turn off the output regulation function; however, if such practice becomes common, the overall system will experience other problems.

The attacks can be generated with much less effort as they require falsification of just one of the sensors at the end of the feeder. The approach was to keep the voltage high at the LRT during the day and hence to switch the tap upward in the morning. This is especially in contrast with the case without the overvoltage protection function, where no damage could be made through attacks on one to two nodes, as we have seen in Table I.

It seems relatively easy to upgrade the detection algorithm so that it can deal with such attacks. The one falsified sensor value behaves quite unnatural and goes so close to the lower limit in the morning hours. Even after one forced tap change occurred, its voltage reading remained low, which was necessary for another tap change to follow.

VII. Conclusion

In this paper, we have studied cyber security issues in distributed systems under centralized voltage regulation. The attacks are made through falsification of sensor measurements sent to the tap controller from sectionizing switches. We have introduced a simple detection algorithm whose parameters can be determined by the system behavior under normal conditions. Due to its simplicity, we could formulate optimization problems for characterizing the most effective attacks against the algorithm. Then, via detailed simulations based on realistic settings, we have demonstrated that falsification in node voltage measurements can be detected if the number of such nodes

is limited. However, a larger number of attacks can result in damage in the form of voltage violation at some nodes. Moreover, we have studied another type of attack which can be harmful to the PV owners since their PVs may produce less output power; though these attacks are less dangerous to the system, this type was found much easier to realize and potentially more problematic if they spread. The obtained results provide us with useful insights which will serve as the basis for further studies.

In the future, we will deal with more complex distribution systems with multiple feeders which may contain loops and also more devices for voltage regulation under the centralized control approach. While the overall regulation becomes more complicated, the basic strategies toward attacks as well as their detection should be based on the findings in this paper. Also, at residences equipped with PVs, one way to avoid PV output power loss is to use storage devices. They may be useful in reducing the influence of cyber attacks. To address the effectiveness of this approach is also left for future work.

Furthermore, it may be of interest to consider the use of sensors in smart meters for the purpose of cyber security of the feeders. The detection method of this paper relies on the assumption that sectionizing switches are equipped with voltage sensors. At nodes such switches are not available, data from smart meters may be useful since they are commonly equipped with voltage sensors and can transmit local information.

REFERENCES

[1] E. Hossain, Z. Han, and H. V. Poor, *Smart Grid Communications and Networking*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[2] Y. Chakhchoukh and H. Ishii, "Cyber attacks scenarios on the measurement function of hybrid state estimation," *IEEE Trans. Power Syst.*, to be published.

[3] M. E. Elkhatib, R. El-Shatshat, and M. M. A. Salama, "Novel coordinated voltage control for smart distribution networks with DG," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 598–605, Dec. 2011.

[4] H. E. Farag, E. F. El-Saadany, and R. Seethapathy, "A two ways communication-based distributed control for voltage regulation in smart distribution feeders," *IEEE Trans. Smart Grid*, vol. 3, no. 1, pp. 271–281, Mar. 2012.

[5] A. M. Giacomoni, S. M. Amin, and B. F. Wollenberg, "A control and communication architecture for a secure and reconfigurable power distribution system: An analysis and case study," in *Proc. 18th IFAC World Congr.*, Milano, Italy, 2011, pp. 1678–1684.

[6] M. Govindarasu and P. W. Bauer, "Special section on keeping the smart grid safe," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 16–17, Jan./Feb. 2012.

[7] Y. Hanai, Y. Hayashi, and J. Matsuki, "Voltage control for loop distribution system with renewable energy sources," in *Proc. Int. Conf. Renew. Energy Power Qual.*, Granada, Spain, 2010, pp. 1–6.

[8] Y. Hayashi, "Development of technology for collaborative energy management system and foundation for versatile demonstrative research and its evaluation," Jpn. Sci. Technol. Agency, Tokyo, Japan, CREST Program, 2012.

[9] Y. Isozaki *et al.*, "On detection of cyber attacks against voltage control in distribution power grids," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Venice, Italy, 2014, pp. 848–853.

[10] D. Kundur *et al.*, "Towards modelling the impact of cyber attacks on a smart grid," *Int. J. Security Netw.*, vol. 6, no. 1, pp. 2–13, 2011.

[11] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Security*, vol. 14, no. 13, pp. 1–33, 2011.

[12] K. Manandinar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[13] Y. Mo *et al.*, "Cyber-physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[14] H. Nishino and H. Ishii, "Distributed detection of cyber attacks and faults for power systems," in *Proc. 18th IFAC World Congr.*, Cape Town, South Africa, 2014, pp. 11932–11937.

[15] 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.

[16] K. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proc. 50th IEEE Conf. Decis. Control*, Orlando, FL, USA, 2011, pp. 4054–4059.

[17] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[18] A. Teixeira *et al.*, "Security of smart distribution grids: Data integrity attacks on integrated Volt/VAR control and countermeasures," in *Proc. Amer. Control Conf.*, Portland, OR, USA, 2014, pp. 4372–4378.

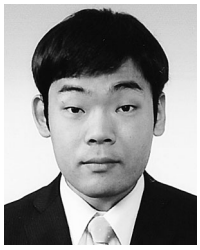
[19] R. Tonkoski, L. A. C. Lopes, and T. H. M. El-Fouly, "Coordinated active power curtailment of grid connected PV inverters for overvoltage prevention," *IEEE Trans. Sustain. Energy*, vol. 2, no. 2, pp. 139–147, Apr. 2011.

[20] Y. Ueda, K. Kurokawa, T. Tanabe, K. Kitamura, and H. Sugihara, "Analysis results of output power loss due to the grid voltage rise in grid-connected photovoltaic power generation systems," *IEEE Trans. Ind. Electron.*, vol. 55, no. 7, pp. 2744–2751, Jul. 2008.

[21] R. A. Walling, R. Saint, R. C. Dugan, and J. Burke, "Summary of distributed resources impact on power delivery systems," *IEEE Trans. Power Del.*, vol. 23, no. 3, pp. 1636–1644, Jul. 2008.

[22] I. Watanabe, K. Masutomi, and I. Ono, "Robust meter placement against false data injection attacks on power system state estimation," in *Proc. ICONIP*, Daegu, Korea, 2013, pp. 569–576.

[23] S. Yoshizawa, Y. Hayashi, M. Tsuji, and E. Kamiya, "Centralized voltage control method of load ratio control transformer and step voltage regulator for bank fault restoration," in *Proc. 3rd IEEE PES Innov. Smart Grid Tech. Europe*, Berlin, Germany, 2012, pp. 1–7.



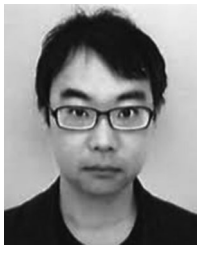
Yasunori Isozaki was born in 1990, in Yokohama, Japan. He received the B.Eng. degree in control systems engineering, and the M.Eng. degree in computational intelligence and systems science from the Tokyo Institute of Technology, Yokohama, in 2013 and 2015, respectively.

He is currently with Toyo Electric Manufacturing Company Ltd., Tokyo, Japan. His current research interests include systems control, distribution systems, and cyber security.

Shinya Yoshizawa (S'12) received the B.E. and M.E. degrees in electrical engineering and bioscience from Waseda University, Tokyo, Japan, in 2011 and 2013, respectively, where he is currently pursuing the Ph.D. degree in engineering.

His current research interests include operation and control of active distribution systems and smart grids.

Mr. Yoshizawa is a Student Member of the IEE of Japan.



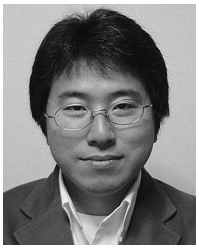
Yu Fujimoto received the Ph.D. degree in engineering from Waseda University, Tokyo, Japan, in 2007.

He is an Associate Professor with the Advanced Collaborative Research Organization for Smart Society, Waseda University. His current research interests include machine learning and statistical data analysis, data mining in energy domains, and especially for controlling power in smart grids.

Hideaki Ishii (M'02–SM'12) received the M.Eng. degree in applied systems science from Kyoto University, Kyoto, Japan, in 1998, and the Ph.D. degree in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 2002.

He was a Postdoctoral Research Associate with the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Champaign, IL, USA, from 2001 to 2004, and a Research Associate with the Department of Information Physics and Computing, University of Tokyo, Tokyo, Japan, from 2004 to 2007. He is currently an Associate Professor with the Department of Computational Intelligence and Systems Science, Tokyo Institute of Technology, Yokohama, Japan. His current research interests include networked control systems, multiagent systems, hybrid systems, cyber security of power systems, and probabilistic algorithms.

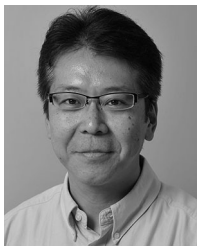
Dr. Ishii has served as an Associate Editor for *Automatica* and previously for the IEEE TRANSACTIONS ON AUTOMATIC CONTROL. He is the Chair of the International Federation of Automatic Control Technical Committee on Networked Systems.



Isao Ono received the B.Eng. degree in control engineering, and the M.Eng. and Dr.Eng. degrees in computational intelligence and systems science from the Tokyo Institute of Technology, Yokohama, Japan, in 1994, 1995, and 1997, respectively.

He was a Postdoctoral Research Associate with the Tokyo Institute of Technology, from 1997 to 1998. He was a Research Associate in 1998, a Lecturer from 1998 to 2001, and an Associate Professor from 2001 to 2005 with the University of Tokushima, Tokushima, Japan. He has been an Associate Professor with the Tokyo Institute of Technology, since 2005. His current research interests include evolutionary computation, optimization, and cyber security.

Prof. Ono is a Member of the Society of Instrument and Control Engineers; the Institute of Systems, Control, and Information Engineers; the Japanese Society for Evolutionary Computation; and the Japanese Society for Artificial Intelligence.



Takashi Onoda received the B.A. degree in science from International Christian University, Mitaka, Japan, in 1986; the M.S. degree in nuclear engineering from the Tokyo Institute of Technology, Yokohama, Japan, in 1988; and the Dr.Eng. degree in mathematical engineering from the University of Tokyo, Tokyo, Japan, in 2000.

He has been affiliated with the Central Research Institute of Electric Power Industry, Tokyo, since 1988. He was a Visiting Researcher with GMD FIRST, Berlin, Germany, from 1997 to 1998. He is currently a Sector Leader with the Central Research Institute of Electric Power Industry. His current research interests include statistical learning theory and its applications.

Dr. Onoda is a Member of the Japanese Society for Artificial Intelligence.

Yasuhiro Hayashi (M'91) received the B.Eng., M.Eng., and Dr.Eng. degrees in electrical engineering from Waseda University, Tokyo, Japan, in 1989, 1991, and 1994, respectively.

In 1994, he became a Research Associate with Ibaraki University, Mito, Japan. In 2000, he became an Associate Professor with the Department of Electrical and Electronics Engineering, Fukui University, Fukui, Japan. He became a Professor with the Department of Electrical Engineering and Bioscience, Waseda University, in 2009. His current research interests include optimization of distribution system operation and planning, power system analysis, and load forecasting.

Prof. Hayashi is a Member of the Institute of Electircal Engineers of Japan and the International Council on Large Electric Systems.