Smart-Grid –Enabled Load and Distributed Generation as a Reactive Resource

Katherine M. Rogers, *Student Member, IEEE,* Ray Klump, *Member, IEEE,* Himanshu Khurana, *Senior Member, IEEE,* Thomas J. Overbye, *Fellow, IEEE*

***Abstract*—At the residential level, devices which are in place now and expected in the future have the ability to provide reactive power support. Inverters which connect distributed generation such as solar panels and pluggable hybrid electric vehicles (PHEVs) to the grid are an example. Such devices are not currently utilized by the power system. We investigate the integration of these end-user reactive-power-capable devices to provide voltage support to the grid via a secure communications infrastructure. We show how to determine effective locations in the transmission system and how to control reactive power resources at those locations. We also discuss how to determine reactive support groups which parallel the regions of the secure communications architecture that is presented. Ultimately, our goal is to present how the Smart Grid can allow the utilization of available end-user devices as a resource to mitigate power system problems such as voltage collapse.**

***Index Terms*— reactive power resources, cyber security, voltage control, linear sensitivity analysis**

I. Introduction

Power system operation is currently contingency-constrained, and often by low-voltage violations. A contingency is a "what if" scenario that utilities use to gauge the operational reliability of the power system. Utilities regularly run a series of contingencies in a process known as contingency analysis. Under normal conditions, the system is operated so that it can withstand the loss of any one element [1] or one credible contingency. The ability of a system to withstand a list of "credible" disturbances or contingencies is defined to be operational reliability, but was previously called security [2]. This means that for any single contingency, the steady-state analysis converges to a solution that does not result in any limit violations in the post contingent system state. However, as power systems become more heavily loaded, they are pushed closer to their operating limits, and this can result in an increase in the number of limit violations and unsolvable contingencies. In the case of an unsolvable contingency, the effects of the real-world outage cannot be modeled by the steady-state power flow equations. However, the effects of the outage can safely be assumed to be undesirable, perhaps leading to a voltage collapse. Voltage collapse is a process whereby voltages progressively decline until it is no longer possible to maintain stable operating voltages [3]. It is well known that available reactive power resources can be used to raise voltages and thus make the system less vulnerable to voltage instability.

Optimal control recommendations can be found to restore the system to a stable state after a disturbance [4]. The type of control which focuses on restoration of an unstable system is called corrective control. Corrective control directs the system to a new stable equilibrium point shortly following a severe disturbance [5], [6]. In contrast, preventative control is carried out before any instability occurs. Such optimal controls are not always practical and may require involvement of a large number of buses in the system. Generator re-dispatch can be classified as corrective control, but it is time-constrained by the ramp limits of the units. Load shedding can also help restore the system, but it is costly and a last resort. Instead, one can choose realistic control actions which are the most effective for the problem and the least costly [7]. The switching of transmission lines has the ability to be used as a corrective control [8]. Since the switching of transmission lines changes the system state, such actions may be applied alleviate voltage problems [9], [10]. Flexible AC Transmission System Devices (FACTS) [11], [12], [13] can also provide corrective control by absorbing or generating reactive power quickly. Synchronous condensers are also a reactive power resource. The key idea is that the established controls may be enacted within an allotted time frame and a secure system state can be restored.

Currently, such control mostly occurs at the substation level. The Smart Grid, enabled by concepts presented in this paper, allows us to consider a more comprehensive form of reactive power control that goes all the way from the transmission system level to the end-user. This paper presents the idea of using as a resource existing and new power system devices which are capable of changing reactive power output and discusses the requirements to control these resources over a secure communications infrastructure. Such controls, made available via smart-grid technologies, can be actuated in the system to maintain a healthy voltage profile. The reactive power resources include inverters on solar panels, pluggable hybrid electric vehicles (PHEVs), and many other distributed sources [14], [15]. Locations in the system where machines or converters are present are all possible reactive power resources for the grid. The power buffer concept [14], [16],

The authors would like to acknowledge the support of the support of NSF through its grant CNS-0524695, the Power System Engineering Research Center (PSERC), and the Grainger Foundation. The authors would like to thank U.S. Congressman Bill Foster who motivated the ideas behind the paper.

The authors are with the University of Illinois Urbana-Champaign, Urbana, IL 61801 (e-mail: krogers6@illinois.edu, klumpra@lewisu.edu, hkhurana@illinois.edu, overbye@illinois.edu,).

[17], allows the power electronics to take advantage of isolation and present a desired behavior to the grid. In the context of this paper, the desired behavior is to provide reactive power injection as needed. These devices can be called upon in a decentralized manner to correct voltage violations in their local area, using secure, authenticated messaging to coordinate the control. That is the vision put forth by this paper.

II. Sensitivity of Voltages to Reactive Power

Sensitivities are linearized relationships which are often used [18] to reveal the impact that a small change of a variable has on the rest of the system. The buses in the system which have loads whose MVAr (Q) output we are attempting to control will be denoted as Q-Controlled (Q-C) buses. The sensitivities of voltages to reactive power injections are fundamental to the analysis of determining locations for and setting reactive power outputs of Q-C buses.

A. Power Flow Equations and Notation

The equations from which the sensitivities are derived are the AC power flow equations for real power P and reactive power Q at a bus *i* stated in (1) and (2),

$$P_{i,calc} = V_i \sum_{j=1}^{n} V_j \left[G_{ij} cos(\theta_i - \theta_j) + B_{ij} sin(\theta_i - \theta_j) \right] \quad (1)$$

$$Q_{i,calc} = V_i \sum_{j=1}^{n} V_j \left[G_{ij} sin(\theta_i - \theta_j) - B_{ij} cos(\theta_i - \theta_j) \right] \quad (2)$$

where n is the number of buses, $\mathbf{s}_{(\theta,V)} = [\boldsymbol{\theta}, \boldsymbol{V}]^T$ is a vector of bus voltage magnitudes and angles, and $\boldsymbol{G}$+j$\boldsymbol{B}$ is the system admittance matrix. Power balance is expressed by the vector $\boldsymbol{f}_{(p,q)} = [\Delta \boldsymbol{p}, \Delta \boldsymbol{q}]^T$ which must equal zero at solution, where $\Delta p_i = P_{i,calc} - (P_{i,gen} - P_{i,load})$, and $\Delta q_i = P_{i,calc} - (Q_{i,gen} - Q_{i,load})$.

B. Power Injection and State Variable Sensitivities

The negative inverse of the power flow Jacobian, $\boldsymbol{J}$, describes the way the state variables $\boldsymbol{\theta}, \boldsymbol{V}$ change in a solution of the power flow due to bus power injection mismatch.

$$\Delta \boldsymbol{s}_{(\theta,V)} = [-\boldsymbol{J}]^{-1} \cdot \boldsymbol{f}_{(p,q)} \quad (3)$$

Let $\boldsymbol{Q_s}$ be the vector of specified net reactive power injections at each bus, so $Q_{s,i} = Q_{i,gen} - Q_{i,load}$. Then, the sensitivity of voltage magnitude $\boldsymbol{V}$ to specified reactive power $\boldsymbol{Q_s}$ is given by the block matrix $\boldsymbol{\Lambda_{VQ}}$ of $\boldsymbol{J}^{-1}$:

$$[\boldsymbol{J}]^{-1} = \begin{bmatrix} \frac{\partial \boldsymbol{\theta}}{\partial \mathbf{P_s}} & \frac{\partial \boldsymbol{\theta}}{\partial \mathbf{Q_s}} \\ \frac{\partial \mathbf{V}}{\partial \mathbf{P_s}} & \frac{\partial \mathbf{V}}{\partial \mathbf{Q_s}} \end{bmatrix} = \begin{bmatrix} \boldsymbol{\Lambda_{\theta P}} & \boldsymbol{\Lambda_{\theta Q}} \\ \boldsymbol{\Lambda_{VP}} & \boldsymbol{\Lambda_{VQ}} \end{bmatrix} \quad (4)$$

The sensitivities $\boldsymbol{\Lambda_{VQ}}$ describe how voltage magnitude state variables change in a solution of the power flow due to a small change in specified reactive power injection at a bus.

III. A Method for Control of Voltages

Effective placement and control of Q-C buses are determined based on the sensitivities given by (4). Classification of loads can further help in selecting the Q-C buses that are the most controllable.

A. Voltage Control Problem

The objective function is given by f_1, the sum of the differences of the bus voltages from their specified values, where M is the number of bus voltages to be controlled:

$$f_1 = \sum_{i=1}^{\boldsymbol{M}} \left[\boldsymbol{V} - \boldsymbol{V}_{spec} \right]_i^2 = \sum_{i=1}^{\boldsymbol{M}} [\boldsymbol{\eta}_i]^2 \quad (5)$$

The voltage control problem is to minimize f_1 subject to the power flow constraints and limits on equipment. That is, the goal is to determine settings at the Q-C buses such that the voltage profile of the system is as close to the specified voltage profile as possible. From optimization theory, there are a number of ways to solve this problem [19]; a comparison of optimization methods is not in the scope of this paper. Here we use the steepest descent approach, and the $\boldsymbol{Q_s}$ values to minimize (5) are solved for using the sensitivities given in (6).

B. Selection of Q-C Buses

Sensitivities can be used to identify buses whose reactive power injections have a high impact on voltages of interest. The buses identified from the sensitivities are candidates for selection as Q-C buses. The sensitivities of f_1 to reactive power injection are given by the following vector:

$$\nabla f_1 = 2\boldsymbol{\eta}\boldsymbol{\Lambda_{VQ}} \quad (6)$$

Buses with higher sensitivities are able to provide more control, whereas buses with sensitivities of zero have no impact on the control objective. The Q-C candidate buses are found by determining the buses with the highest magnitude sensitivities for the objective function f_1. That is, the k most effective locations correspond to the k elements of the sensitivity vector (6) which are furthest from zero.

C. Classification of Loads

The controllability of the reactive component of loads can be classified. Since power systems have many load buses, classification can help incorporate knowledge about differing levels of reactive power control capability, and this will improve the selection process for Q-C buses.

Let CAT1 be the most controllable category and CATN be the category that is not controllable at all. A load category can be assigned to each load based on prior knowledge perhaps by the manufacturer or by the engineer performing the analysis. Thus, load categories are an additional factor that can be considered when selecting effective locations for Q-C buses. Loads that are highly controllable (lower category number) should be given a higher priority in the selection of Q-C buses. These load classifications are fluid. For example, as a CAT1 load begins to reach the limits of the reactive power it can supply or absorb, it will switch to a higher-numbered category. Future work will investigate non-heuristic ways to do this reclassification.

IV. Reactive Support Groups

To control voltage by adjusting loads and sources requires communicating control commands efficiently and securely.

The issues involved in achieving this level of communication as well as an example architecture will be presented in Section VI. Ensuring that the communication is efficient and secure can be made easier by focusing the control effort on a subset of the controllers. Rather than consider all devices as potential destinations for reactive control messages, each node will be associated with a reactive support group that consists of the devices that have been determined *a priori* from a recent system model to have the greatest potential to control the affected node's voltage. This section describes various ways to determine the makeup of the reactive support group for a particular node. Similar work has been done [20], [21], [22], [23], [24], [25] to help gauge a system's proximity to voltage collapse.

A. Identify Supporters for each Voltage

Supporter buses can be identified for each voltage. To do this, we go through each row of $\mathbf{\Lambda_{VQ}}$ corresponding to each voltage and determine the l highest values in the row. Since each row is a bus voltage and each column is a reactive power injection, the l highest-magnitude columns for a row give the l best Q-C supporters for that bus's voltage. This method provides a lot of redundancy since if there are m voltages of interest, there will be m reactive support groups where each region has l elements. Ensuring that each voltage has l supporters may be beneficial since we want reactive control groups to be at least some minimal size.

B. Hierarchical Clustering Algorithm

We can also cluster the rows of $\mathbf{\Lambda_{VQ}}$ to identify voltages which are affected similarly by reactive power injections at possible Q-C buses. Hierarchical clustering is one possible approach [26] that may complement well the nature of the communications and security aspects of the problem since the granularity of control ranges from the transmission network to the distribution network end-user. Hierarchical methods called agglomerative schemes begin at the lowest level, with each element as a single cluster, and then, at each increasing level, the closest clusters are merged. Thus, each level represents a different amount of granularity between the clusters. We can slice the hierarchy at different levels depending on how coarse or fine we want the clusters to be. The higher the level, the coarser the grouping becomes. At the highest level, all elements are in one cluster.

Agglomerative clustering relies on the use of a distance matrix $\boldsymbol{D}$. Elements D_{ij} give the distance between row i and j of $\mathbf{\Lambda_{VQ}}$. Any measure of distance may be used; here we use Euclidean distance. At each level, we find the most similar pair of clusters *(r)* and *(s)* by finding the minimum value D_{rs} in the current distance matrix. Then, clusters *(r)* and *(s)* are merged into one cluster. The rows and columns for *(r)* and *(s)* in the distance matrix are deleted and a new row is added for the new cluster *(r,s)*. Any metric can be used to determine the distance of the new cluster *(r,s)* to each other cluster l, but typically the metric is $D_{(r,s)l} = \min(D_{rl}, D_{sl})$. That is, the distance between any two clusters is given by the minimum distance between any two elements of the clusters.

C. Quality-Threshold (QT) Clustering Algorithm

The Quality Threshold (QT) algorithm [26] can also be used to cluster the rows of $\mathbf{\Lambda_{VQ}}$. This method also uses the distance matrix $\boldsymbol{D}$. A threshold and a maximum cluster size are specified initially. For each row of $\mathbf{\Lambda_{VQ}}$, we build a candidate cluster that contains all other rows of $\mathbf{\Lambda_{VQ}}$ which are closer in distance than the threshold. The candidate cluster with the most elements becomes a true cluster. All the points in the true cluster are removed from further consideration. The process then iterates until all points belong to a true cluster.

D. Voltage Coupling Index (VCI) Algorithm

The Voltage Coupling Index (VCI) algorithm also forms groups of voltages that respond the same way to reactive power control. A metric called the flow coupling index is introduced in [27] and is used to describe the ability of line flows to be controlled independently. The same metric can be applied to the control of voltages by reactive power injections, and the metric is then called the voltage coupling index (VCI). The cosine of the angle between two row vectors $\boldsymbol{v_1}$ and $\boldsymbol{v_2}$,

$$cos\theta_{v_1 v_2} = \frac{\boldsymbol{v_1} \cdot \boldsymbol{v_2}}{\|\boldsymbol{v_1}\|\|\boldsymbol{v_2}\|} \qquad (7)$$

of $\mathbf{\Lambda_{VQ}}$ is the VCI. The VCI has values between -1 and 1. When the VCI has an absolute value of 1, the angle between the vectors is zero, and there is complete correlation, either positive or negative, between the ways the two bus voltages respond to control via reactive power injection. When the VCI is zero, the row vectors of $\mathbf{\Lambda_{VQ}}$ are orthogonal, and the voltages have the ability to be independently controlled. The coupling of the control of voltages is important to understand so that attempts are not made to independently control voltages which are highly coupled.

Suppose we form a matrix $\boldsymbol{K}$ where elements K_{ij} give the VCI between voltages represented by rows i and j. The VCI algorithm groups together voltages that are highly coupled with other voltages in the group. The algorithm goes through each row of $\boldsymbol{K}$ and identifies all voltages that are coupled by a VCI with magnitude greater than a threshold. Let this group be A_i, denoted a weak cluster. Then, the algorithm goes through rows of $\boldsymbol{K}$ given by the elements of A_i and identifies voltages with coupling indices above the threshold and places them in the group A_j. If all the elements in A_i and A_j match, the set of matching elements is identified as a strong cluster.

Note that in this algorithm, it is possible for a bus not to belong to any strong cluster. The number of buses in a cluster is a function of the chosen threshold. However, buses that do not belong to a cluster will be identified as weak clusters containing only themselves. The interpretation is that voltages in strong clusters are good candidates for the reactive support groups, but weak clusters may need to be used to ensure that all buses are included in a group.

E. Hybrid Approach

The most thorough approach to choosing voltage control groups may be a combination of algorithms. For example, the VCI algorithm can be applied first to determine the voltage coupling groups. Then, a number of l supporters can be found for each group. This would ensure that each region would always be able to receive enough reactive power support by building in redundancy.

V. Reactive Power Control Test Cases

We illustrate how locations for Q-C buses can be chosen and how Q-C buses can be controlled to improve voltage profile, including the selection of reactive support groups. The methodology presented previously in the paper is applied, and we discuss the results and their implications.

A. IEEE 24-Bus Reliability Test System (RTS)

We consider the IEEE 24-Bus Reliability Test System (RTS) [28] as our study system. A one-line diagram for the system is shown in Figure 1. The RTS has low voltages around 0.95 per unit. The lowest voltages in the system are at buses 3,4,8,9, and 24.

Suppose that the controllability of loads can be classified into categories as in Section III. For simplicity, we consider only two categories here; CAT 1 contains the loads which are completely controllable, and CAT3 contains the loads which are not controllable at all. The only CAT3 buses in the RTS are buses 11, 12, and 17 since these have reactive power loads of zero. The category labels can easily be changed as desired. Since CAT1 loads have the ability to be controlled, they are allowed to be selected as Q-C buses. Which CAT1 buses are selected is based on the sensitivities as discussed in Section III. Note that a CAT2 classification would contain partially-controllable loads, but a mixture of different controllability levels is not considered at this time.

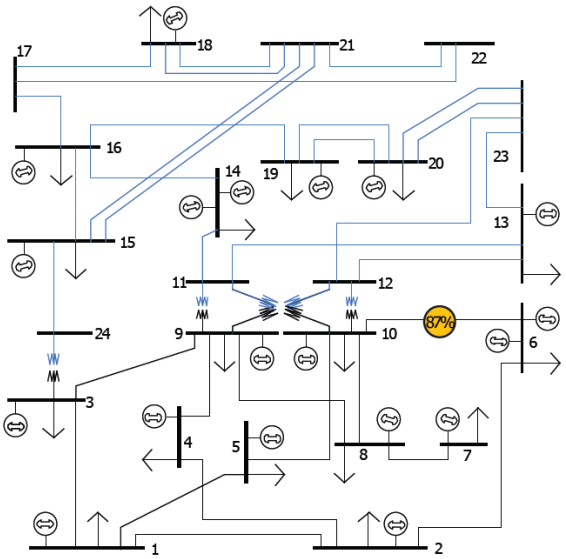

Figure 1. IEEE 24-Bus RTS

If we consider the four most effective CAT1 locations as Q-C buses to raise the five lowest voltages to a voltage profile of 1 per unit, the required net MVAr outputs (Q_{net}) to achieve this control are determined (columns 2 and 3 of Table 1).

Table 1. RTS voltage improvement

Bus #	Initial Q_{net}	Final Q_{net}	Initial voltage	Final voltage
3	-37 MVAr	37 MVAr	0.9469	1.0057
4	-15 MVAr	15 MVAr	0.9598	1.0022
8	-35 MVAr	35 MVAr	0.9593	0.9975
9	-36 MVAr	36 MVAr	0.9603	1.0050
24			0.9594	0.9852

A negative Q_{net} indicates a net reactive power load while a positive Q_{net} indicates a source. To achieve the voltage correction, the power factors at all Q-C buses became leading instead of lagging. Columns 4 and 5 of Table 1 show the voltages at the low-voltage buses, and overall system voltages are shown in Figure 2.

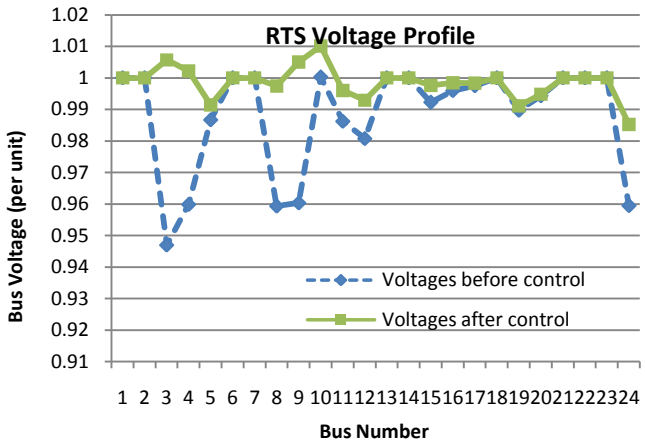

Figure 2. RTS voltage profiles

Reactive power adjustment at a small number of buses can cause a substantial improvement of the overall voltage profile. The use of reactive-only controls as opposed to other forms of corrective control has the advantage that such controllers are already available in the system but not being utilized, and more are likely to be added. Also, the use of reactive power controls may prevent the need to shed load or change generation output as a corrective control.

In this example, the five worst voltages completely overlap the four most effective CAT1 locations. As systems become more heavily loaded, the two groups will likely no longer overlap, as the lowest-voltage buses will no longer be CAT 1 because they will no longer have reserves. Furthermore, at high load levels, the response will likely no longer be so linear, making it more difficult to determine the proper size for the adjustments. Nevertheless, the approach will identify the most effective supports to deploy, and additional adjustments can be made if needed until the desired voltage levels are reached.

B. Linear Estimate of the Control

In the scenario above, we solved for the Q values needed to achieve the desired voltage profile within a small tolerance. We can also directly use the sensitivities to approximate the control needed, which requires no iteration. The accuracy of the control is dependent on the linearity of the relationship between the reactive power at the Q-C buses and the voltages.

In Table 2, the linear approximation of the controls needed is compared to the actual controls. The linear estimates of Q_{net} at buses 3 and 4 are close to the actual values, but buses 8 and 9 are not. Using the Q_{net} values from the linear estimate, the voltages at the low-voltage buses V_{ESTQ} are given in column 6 of Table 2. The final voltages V_F of Table 1 are also shown. With both controls, the voltage profile was substantially improved, but the improvement was not as great with the linear approximation. However, the approximation can most likely be calculated a lot faster, so the discrepancies in the final voltage values may be tolerable.

Table 2. RTS linear control estimate

Bus #	Q_{net} Needed	Q_{net} Estimated	% Error	V_F	V_{ESTQ}
3	37 MVAr	37.26 MVAr	0.69 %	1.0057	1.00294
4	15 MVAr	14.52 MVAr	3.21 %	1.0022	0.9982
8	35 MVAr	41.69 MVAr	19.11%	0.9975	0.99813
9	36 MVAr	13.01 MVAr	63.86%	1.0050	0.99826
24				0.9852	0.98396

C. *Reactive Support Groups*

Applying the algorithms described in Section IV to the RTS, we determine possible reactive support groups. For the agglomerative scheme, the clusters form as shown in Figure 3. From Figure 3, we can see that the hierarchical algorithm initially forms clusters containing (11,12) and (17,20). Then, a large cluster forms and begins to grow. At a higher level, a cluster forms containing (3,24), but then that cluster is absorbed into the large cluster. The last buses to join any cluster are buses 3, 4, 5, 8, 9, and 24.

For the QT algorithm, with a threshold of 0.04 and a maximum cluster size of five, the clusters are given by column 1 of Table 3. The QT algorithm shows similar results to the hierarchical algorithm. Buses which were the last to join a cluster in the hierarchical method are shown by the QT algorithm to be their own cluster. The rest of the buses are in two groups. However, if the maximum cluster size is increased to eight instead of five, the buses in the second cluster become part of the large group, which coincides with the large group we saw form in the hierarchical method.

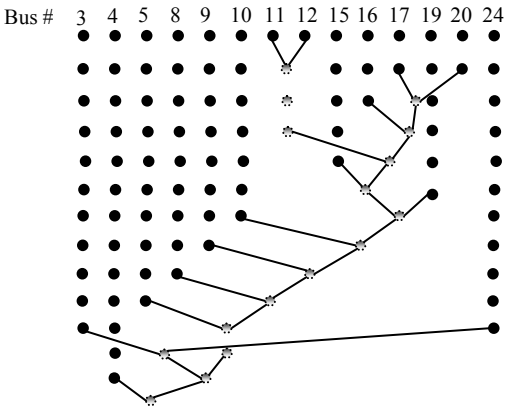

Figure 3. Progression of hierarchical clustering

Using the VCI algorithm, strong and weak voltage coupling clusters are identified in columns 2 and 3 of Table 3. The same bus may belong to multiple strong clusters, so some regions overlap. Voltages which are not coupled to any other voltages form their own weak cluster.

Table 3. RTS clusters, each shown in brackets

QT	VCI - Strong	VCI - Weak
[3], [4],[5],[8],[9],[24]	[9,11,12]	[4],[5],[8]
[10, 12, 11, 17, 20]	[15,16,17]	[3,24],[3,15,24]
[15, 16, 19]	[16,17,19]	[9,11,12],[10,11,12]
	[19,20]	[9,10,11,12]
	[3, 24]	[15,16,17,24]
		[15,16,17,19], [19,20]

Based on the strong clusters of the VCI algorithm and the additional buses 4, 5, 8, and 10 we can identify for each group *l* supportive buses. Supporting buses may only be CAT1 buses. Let *l*=5; each region's five most supporting buses are given by column 2 of Table 4, in order of decreasing support effectiveness:

Table 4. Supports for Voltage Groups

Voltage-Coupled Groups	5 Supporter Buses
4	[4,9,3,8,24]
5	[5,10,8,9,4]
8	[8,9,10,4,3]
10	[12, 15, 11, 17,3]
[9,11,12]	[9,4,10,3,8]
[15,16,17]	[15,16,19,24,3]
[16,17,19]	[16,19,15,24,3]
[19,20]	[19,20,16,15,24]
[3, 24]	[3,24,9,15,4]

The hybrid approach of Table 4 uses information we know about how voltages can be controlled with respect to other voltages and also ensures that each bus voltage will have at least *l* supporters. Using only one clustering algorithm may leave some voltages without any supporters (buses 4,5, and 8).

D. *August 14, 2003 Blackout*

The August 14, 2003 blackout report [3] states that a lack of adequate dynamic reactive reserves with a lack of knowledge about critical voltages and maximum import capability left the Cleveland-Akron area in a vulnerable state. Although the system was secure, the Cleveland-Akron area was highly vulnerable to voltage instability problems. The area had little reactive margin and few relief actions available to operators in the face of contingencies. Early in the afternoon of August 14, First Energy operators began requesting capacitors be put in service, additional voltage support from generators, and transformer tap changes. The low voltages contoured at the top of Figure 4 give a reconstructed state of the system prior to the blackout, and the bottom of Figure 4 shows the voltages after correcting the power factor at just five buses to unity power factor. According to [3], inadequate reactive power supply was a factor in most previous major North American blackouts.

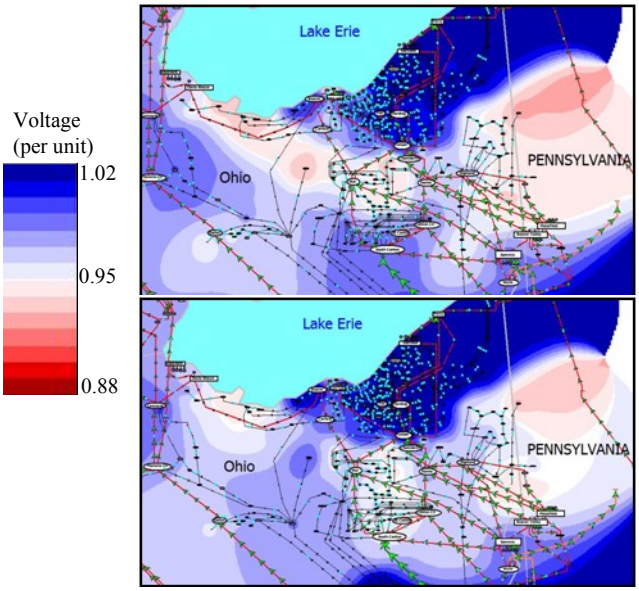

Figure 4. Voltage contours, before (upper) and after (lower)

VI. Secure Communications Cyber Infrastructure

Distributed reactive power control requires the delivery of messages between devices and controllers in a timely and secure manner. Timeliness is needed to support the tens-of-seconds to minutes voltage time-scales while cyber security is needed to ensure that adversaries cannot use the cyber infrastructure to cause harm. From the set of standard cyber security properties of confidentiality, integrity, and availability, it is the latter two that are most important for this application. It is far more important to ensure that only authentic messages are delivered (integrity) and that all authentic messages are delivered (availability) than to ensure that no one eavesdrop.

Authentication is an exceptionally important property for distributed reactive power control applications, since incorrect responses of the controllers can have disastrous consequences for the system. That is, if distributed reactive power resources can restore an unsolvable system to solvability, then they could also do the opposite. Authentication protocols can address this challenge by using cryptographic primitives and key material in their design. Availability is crucial because otherwise the controllers may not be able to reach devices to provide control, or worse, they may think that their messages are being delivered when they are not. Availability can be provided by adequate monitoring of the network to ensure its overall health and correct operation as well as by designing redundancy into the network architecture.

In this section, we explore various approaches for authentication and availability identifying their benefits and drawbacks. A more comprehensive analysis that identifies an optimal solution is left as the subject of future work. In our discussion we use the simplified view of the network between a controller and a device for two-way communication shown in Figure 5:

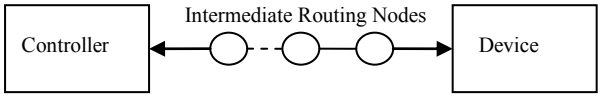

Figure 5: Network path between a controller and a device

Intermediate network nodes may be wired/wireless routers or other devices and controllers that offer message-relaying capabilities. In the emerging Smart Grid, a variety of networking tools and technologies is likely to be realized. These include traditional fiber-based networks, cellular network, Wi-Fi and Wi-Max networks as well as more ad-hoc radio and wireless mesh networks. The goal is to provide end-to-end authentication between the control and device even when intermediated routing nodes are not fully trusted.

A. Authentication

Authentication mechanisms are used to "corroborate that an entity is the one that is claimed" according to the international standard ISO/IEC 9798-1 [29]. These mechanisms are typically constructed using cryptographic tools such as encryption, message authentication codes (e.g., SHA-1), HMACs, symmetric cryptosystems (e.g., AES) and asymmetric cryptosystems (e.g., RSA). They are designed to address cyber attacks such as man-in-the-middle attacks, impersonation, forgery and modification. Furthermore, they are designed to provide protocol goodness properties such as replay prevention, message freshness, and complete and effective state management. Authentication protocols can be surprisingly hard to design and [30] identifies key design principles that have been developed specifically for power grid cyber protocols.

Driven by efficiency needs, underlying communication channels, and specific security properties, authentication protocols can be constructed from symmetric or asymmetric cryptosystems. Symmetric key systems are typically more efficient in terms of their computation and communication overheads. For example, several authentication protocols have been developed in the literature that employ 1) HMACs such as SHA-256 HMAC for integrity and authentication, 2) symmetric encryption such as AES for key distribution and management. Asymmetric key systems typically simplify key management and can also provide non-repudiation when needed. For example, there are several authentication protocols developed in the literature that employ digital signatures for integrity and authentication and a public key infrastructure for key distribution.

One of the more challenging attacks that authentication protocols must address is the replay attack. For example, in Figure 5, an adversary may be able to capture messages and replay them to the devices at a later point in time. A replayed message such as "increase reactive power output by 10 MVAr" can have disastrous consequences if accepted. Using message freshness guarantees can prevent replay attacks. There are three common ways of achieving this. If the system can support the notion of time and at least loose clock synchronization then timestamps can provide freshness. That said, timestamps do have their own challenges [31]. Other options include the use of nonces (random numbers) and sequence numbers. Nonces involve extra message exchange while sequence numbers need reliable communication channels to ensure synchronization. ISO/IEC have standardized a few protocols that satisfy varying needs and environments of use [29].

B. Availability

Ensuring system availability is a high priority in critical systems like the Smart Grid which requires that several key issues be addressed. First, the system must be efficient in its use of computation and communication resources so that resources do not get overwhelmed and all requests can be handled. Second, the system must have good error management built in to ensure proper handling of failures (e.g., those resulting from bad messages). Furthermore, the error management functions must be fail-safe in nature so they do not themselves lead to resource exhaustion even in the face of adversarial action. Third, the system must have adequate redundancy built into it so that, if sub-systems fail or are compromised, then the entire system does not collapse. Fourth, the system should support auxiliary security functions that may be deployed in the grid cyber system to detect to and respond to cyber attacks.

C. An Example Communication Exchange

When a node's voltage starts to violate a limit, reactive supports must act to correct it. Section IV described various

ways to identify groups of reactive supports that are likely to be most effective in helping the violating voltage back to acceptable levels. If the reactive support group for each node is held fixed, which is a reasonable decision if the groups are chosen to include all likely supports, then the network of devices that must be coordinated will be known *a priori*. Thus, webs of trust may be established ahead of time, which will greatly simplify the task of distributing the keys to perform authentication.

The system shown in Figure 6 uses a public key infrastructure to provide authentication, a timestamp to certify timeliness, and a hash function to verify message integrity. In this figure, a controller, which may be the node with the voltage violation or some supervisory entity in charge of protecting the nodes under its authority from voltage violations, sends a message to a device within the violated node's reactive support group, and the device responds. The controller will engage in this kind of communication with every device that is part of the violated node's reactive support group. The controller has its own private key PR_C and corresponding public key PU_C, and the controller maintains a list of the public keys of the reactive support group's devices. Each reactive support device has its own private key PR_D and corresponding public key PU_D. Each reactive support device knows the public key PU_C of the controller. The public keys may be distributed *a priori* in a variety of ways similar to what is done for internet communications, including through a public key registry or by a certificate authority. The scale of the key distribution effort will be reduced by limiting the distribution of keys to the members of the reactive support group.

Figure 6. Example communication exchange

When the controller needs to send a particular voltage control command M_{comm} to a device, it sends it in plaintext along with a timestamp that is used to prevent replay. It also signs the message and sends the signature to the device; this is the $Sign(H(M_{comm}|T)_{PRC}$ part of the message. The signature will be used to authenticate the message as coming from the controller instead of a "man in the middle," because only the controller's public key will be able to decipher the message properly if it was indeed signed using the controller's private key, which only the controller should have. It will also be used to verify that no one meddled with the message or that it was otherwise distorted in transit, because the device will be able to decrypt it with the controller's public key PU_C, and compare the decrypted message with the hash $H(M_{comm} \mid T)$ it computes. If the hash matches the decrypted payload, then it knows that (a) only the controller could have sent the message, assuming that no one has stolen its private key, and (b) the message has not been altered in transit.

The timestamp helps ensure the message will not be replayed. When the controller sends the command M_{comm} to the device, it sends along with it the time that it was sent. The controller will store the timestamp in its list L_{req} of timestamps for pending requests. This list helps the controller keep track of which of its requests have been processed. When the device receives the command and timestamp, responds to the command, and then communicates its response to the controller, it sends the same timestamp to the controller, and it records the timestamp in a list L_{proc} of timestamps of already processed requests. When the controller receives the device's response and timestamp T, it will remove the timestamp T from L_{req}. If the device later receives a message with the same timestamp, it will observe from its L_{proc} list that it has already seen this request and that it must be a replay. Therefore, it will safely ignore it.

The same effect could be achieved using nonces instead of timestamps, except that, in order to ensure freshness, the device would have to generate and send the nonce in advance leading to more rounds of communication. Since these devices will likely have the ability to note the time, and since the timing of commands is important, timestamps are a reasonable technique to use to thwart replay attacks.

VII. Conclusion

This paper presents the use of the Smart Grid to allow the coordination of multiple reactive power devices to achieve a control objective, in particular, to restore system voltages. Although the focus of this paper is on system voltages, a similar framework can be developed for other control objectives.

Some reactive power controllable devices at the residential level already exist in the system, and the number is likely to increase as more power electronics are introduced to integrate efficient distributed generation sources. Distributed reactive power can be utilized via a framework like that which is presented in this paper. As new inverter devices with controllable reactive power output are introduced into the grid, these can easily fit into the same framework and add to the reactive power control capability of the system. Thus, distributed reactive power resources can aid in providing widespread, secure, and versatile control of power systems.

VIII. References

[1] North American Electric Reliability Corporation, "Reliability standards for the bulk power systems of North America," July 2008. [Online]. Available: http://www.nerc.com/files/Reliability_Standards_Complete_Set_21Jul08.pdf

[2] N. Balu et al., "On-line power system security analysis," *Proceedings of the IEEE*, vol.80, no.2, pp.262-282, Feb 1992.

[3] U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," April 2004, [Online]. Available: https://reports.energy.gov/BlackoutFinal-Web.pdf

[4] T. J. Overbye, "A power flow measure for unsolvable cases," *IEEE Transactions on Power Systems*, vol. 9, no. 3, Aug. 1994.

[5] T.J. Overbye and R.P. Klump. "Determination of emergency power system voltage control actions." *IEEE Transactions on Power Systems*. vol. PWRS-13. February 1998. pp. 205-210.

[6] Z. Feng, V. Ajjarapu, D. J. Maratukulam, "A comprehensive approach for preventive and corrective control to mitigate voltage collapse," *IEEE Transactions on Power Systems*, vol.15, no.2, May 2000.

[7] T. J. Overbye, “Computation of a practical method to restore power flow solvability,” *IEEE Transactions on Power Systems*, vol. 10, no. 1, pp. 280-287, Feb. 1995.
[8] J. G. Rolim, L. J. Machado, “A study of the use of corrective switching in transmission systems,” *IEEE Transactions on Power Systems*, vol. 10, no. 1, pp. 336-341, Feb. 1999.
[9] K. W. Hedman, R. P. O’Neill, E. B. Fisher, S. S. Oren, “Optimal transmission switching with contingency analysis,” *IEEE Transactions on Power Systems*, vol. 24, no. 3, Aug. 2009.
[10] A. A. Mazi, B. F. Wollenberg, M. H. Hesse, "Corrective Control of Power System Flows by Line and Bus-Bar Switching," *IEEE Transactions on Power Systems*, vol.1, no.3, pp.258-264, Aug. 1986.
[11] K. Ma, J. Mutale, “Risk and reliability worth assessment of power systems under corrective control,” *Proceedings of 41st North American Power Symposium*, Oct. 2009.
[12] W. Shao, V. Vittal, "LP-Based OPF for Corrective FACTS Control to Relieve Overloads and Voltage Violations," *IEEE Transactions on Power Systems*, vol.21, no.4, pp.1832-1839, Nov. 2006.
[13] Hingorani, N.G., "Flexible AC transmission," *Spectrum, IEEE* , vol.30, no.4, pp.40-45, Apr 1993.
[14] D. L. Logue, P. T. Krein, "Utility distributed reactive power control using correlation techniques," *Applied Power Electronics Conference and Exposition, 2001. APEC 2001. Sixteenth Annual IEEE*, vol.2, pp.1294-1300 vol.2, 2001.
[15] M. Begovic, A. Pregelj, A. Rohatgi, D. Novosel, “Impact of renewable distributed generation on power systems,” *Proceedingsof the Hawaii International Conference on System Sciences*, 2001
[16] D. Logue, P. T. Krein, "The power buffer concept for utility load decoupling," *Power Electronics Specialists Conference, 2000. PESC 00. 2000 IEEE 31st Annual* , vol.2, pp.973-978 vol.2, 2000.
[17] W. W. Weaver, P. T. Krein, "Mitigation of power system collapse through active dynamic buffers," *Power Electronics Specialists Conference, 2004. PESC 04. 2004 IEEE 35th Annual*, vol.2, pp. 1080-1084 Vol.2, 20-25 June 2004.
[18] O. Alsac, J. Bright, M. Prais, B. Stott, “Further Developments in LP-Based Optimal Power Flow,” *IEEE Transactions on Power Systems*, Vol. 5, No. 3, Aug 1990, p 697 - 711.
[19] D. G. Luenberger, *Linear and Nonlinear Programming*, 2nd ed, Kluwer Academic Publishers Group, 2003.
[20] R. Navarro-Perez, et al., "Voltage Collapse Proximity Analysis Using Reactive Area Identification", 1988.
[21] Schlueter et al., "A Fast Accurate Method for Midterm Transient Stability Simulation of Voltage Collapse in Power Systems," Decision and Control 1989 28th Annual Conference, Dec. 1989, pp. 340-344.
[22] Chen et al., "Security Analysis for Voltage Problems using a Reduced Model", *IEEE Trans. on Power Systems*, vol. 5, No. 3, Aug. 1990, pp. 933-940.
[23] R. A. Schlueter, et al., "Methods For Determining Proximity To Volt. Collapse", *IEEE Trans. on Power Systems*, vol. 6, No. 2, pp. 258-292, Feb. 1991.
[24] D. G. Taylor, et al., "A Reactive Contingency Analysis Algorithm Using MW and MVAR Distribution Factors", IEEE Power Engineering Society, SP 89-149, Jul. 1989.
[25] R. A. Schlueter, M. W. Chang, A. Costi, "Loss of voltage controllability as a cause for voltage collapse." *Proceedings of the 27th IEEE Conference on Decision and Control*, Paper FP2-5:00, Austin, TX. December 1988.
[26] P. Tan, M. Steinbach, V. Kumar, *Introduction to Data Mining*, Addison Wesley, 2006.
[27] K. M. Rogers, T. J. Overbye, “Power Flow Control with Distributed Flexible AC Transmission System (D-FACTS) Devices,” *Proceedings of 41st North American Power Symposium*, Oct. 2009.
[28] P. M. Subcommittee, "IEEE Reliability Test System," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-98, no. 6, pp. 2047-2054, Nov. 1979.
[29] International Standards Organization and International Electrotechnical Commission. ISO/IEC 9798-1:1997 Information technology – Security techniques – Entity authentication – Parts.
[30] H. Khurana, R. Bobba, T. Yardley, P. Agarwal E. Heine. “Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols,” to appear in *Proceedings of the Forty-Third Annual Hawaii International Conference on System Sciences*, Hawaii, January, 2010.
[31] R. J. Anderson, R. M. Needham, “Robustness principles for public key protocols,” in CRYPTO ’95: *Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology*, pages 236–247, London, UK, 1995. Springer-Verlag.

Katherine M. Rogers (S’05) received the B.S. degree in electrical engineering from the University of Texas at Austin in 2007 and the M.S. degree from the University of Illinois Urbana-Champaign in 2009 and is currently working toward the Ph.D. degree at the University of Illinois Urbana-Champaign. Her interests include sensitivity analysis, power system analysis, and power system protection.

Ray Klump received his BS, MS, and Ph.D. in electrical engineering from the University of Illinois at Urbana-Champaign. He is currently Associate Professor of Mathematics and Computer Science at Lewis University and a Visiting Research Associate Professor at the Information Trust Institute at Illinois. His current research interests include power system stability and smart grid security.

Himanshu Khurana received his MS and PhD from the University of Maryland, College Park in 1999 and 2002 respectively. He is currently a Principal Research Scientist at the Information Trust Institute and a Research Assistant Professor in the Department of Computer Science at the University of Illinois, Urbana-Champaign. His research interests lie in the area of distributed system security, especially as applied to large-scale distributed systems and critical infrastructures.

Thomas J. Overbye (S’87-M’92-SM’96-F’05) received the B.S., M.S. and Ph.D. degrees in electrical engineering from the University of Wisconsin-Madison. He is currently the Fox Family Professor of Electrical and Computer Engineering at the University of Illinois Urbana-Champaign. He was with Madison Gas and Electric Company, Madison, WI, from 1983-1991. His current research interests include power system visualization, power system analysis, and computer applications in power systems.