Table of Contents

Information Flow Analysis of a Load Balancing Implementation for Energy Management in a Smart Grid

Ravi Akella * and Bruce M. McMillin

Department of Computer Science
Missouri University of Science and Technology
Rolla, Missouri 65409-0350, United States
Phone: +1(573)341-6435 Fax: +1(573)341-4501
{rcaq5c, ff}@mst.edu

Abstract. Information flow security within the context of multilevel security deals with ways to avoid unwanted information flow from a high level domain to a low level domain. Several confidentiality and information flow properties were formalized in literature. However, applying them to Cyber-Physical Systems (CPSs) uncovers aspects such as causality, non-determinism, time, and probability which add to the challenge of protecting the confidentiality. This paper performs an information flow analysis of a future power system which is a CPS with complex information flow and confidentiality requirements. A distributed power balancing scheme implemented for optimal utilization of resources in an advanced smart grid, is the model CPS used. Confidentiality properties such as non-deducibility, and a few of its extensions, are analyzed in this paper by directly applying them to the infrastructure considered. The proposed approach provides a unique direction for formalizing information flow properties for such systems with inherent complexity and security requirements.

Key words: Security, Information Flow, Confidentiality, Cyber-physical system, CSP, Non-inference, Bisimulation based Non-deducibility on Compositions, Load balancing

1 Introduction

Information flow analysis of a system reveals the design and implementation issues that divulge its confidentiality. Confidentiality is usually regarded as being violated when there is an information flow from a high level domain to the low level domain. Non-interference [1], Non-deducibility [2] and their extensions to

* This work was supported in part by the Future Renewable Electric Energy Distribution Management Center; a National Science Foundation supported Engineering Research Center, under grant NSF EEC-0812121 and NSF CSR award CCF-0614633.

information flow properties [3] [4] [5] are concerned with preventing information from being downgraded through covert channels and other such potential causes. This paper extends the application of these information flow properties to more complex Cyber-Physical Systems (CPSs) which are integrations of physical and computational processes. Information flow analysis in CPSs is made more complex by inherently observable cyber and physical events, any of which may divulge confidentiality within the system. Aspects of time, non-determinism, probability, topology and the semantics of the underlying physical system add to unintended information flow are hard to model and add to the complexity of potential confidentiality and integrity violations.

Of particular interest are modern "Smart Grid" systems. Smart grid is a term that embraces many concepts, from smart metering, to smart distribution, to smart transmission systems [6–8]. The economics and power management of such microgrids are only beginning to be understood [9] [10]. While dynamic distribution of energy and protection in micro grids involving control strategies within the system was discussed in [11] [12], less attention has been paid to system security properties, and, in particular, confidentiality properties. This paper addresses confidentiality properties based on information flow analysis with respect to an observer being able to infer about or interfere with the actions that take place within asmart gridSmart power meters, as a first Smart Grid step, are being installed in the United States to both monitor and control energy usage. Such systems are not without security concerns, however [13]. A recent MSNBC article pointed out a potential risk of this increased monitoring, "Would you sign up for a discount with your power company in exchange for surrendering control of your thermostat? What if it means that, one day, your auto insurance company will know that you regularly arrive home on weekends at 2:15 a.m., just after the bars close? " [14]. The result from tying cyber systems with physical systems open up a new realm of the privacy and confidentiality issues. Continuing forward with regard to renewable energy resources, consider the case of two neighbors Fred and Barney who agree to each purchase a renewable resource, and then share their power output as shown in Figure 1.

Fred purchases a windmill (Wind Turbine) and Barney purchases a Solar Panel (Photvoltaic Array). When the sun shines, Barney‘s power is used by both, when the wind blows, Fred‘s power is used by both. When there is excess, they agree to sell it back to the electric utility grid for a profit. The system operates well for a while and both Fred and Barney are satisfied as they enjoy reduced energy costs.

Fred, however, gets greedy and doesn't necessarily want Barney to share in these profits, so he also buys a battery. Fred now changes the operation of his system; when the wind blows, he sends the excess to his battery. Later, at a time of economic opportunity, he sells this stored energy back to the utility. Barney becomes suspicious of Fred and sneaks over and monitors Fred's power transfer to the utility (over Fred's power line coming into his house). Barney also monitors his own power line and observes that he is drawing power from the utility, Fred is not providing power, but Fred's wind turbine is spinning. From

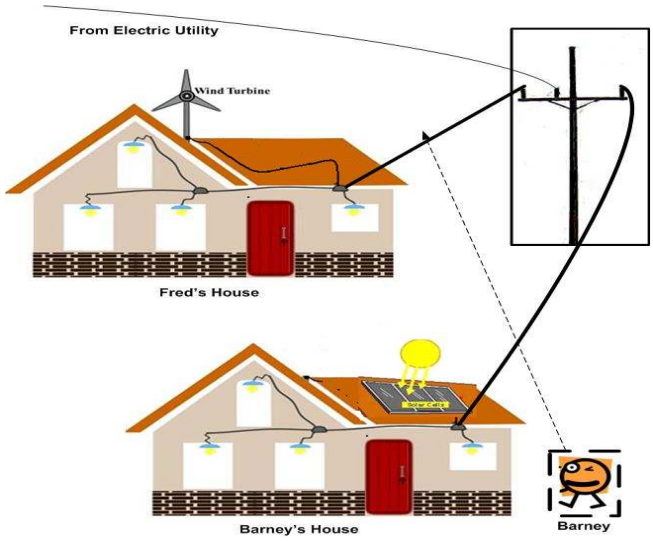

Fig. 1. A Simple Case of Information Flow

Barney's point of view, since he doesn't know about the battery, Fred's power transfer is consistent with Fred using all the power he generates. Thus, Fred's actions are completely hidden from Barney. Fred, however, monitor's Barney's power, and when Barney is not drawing power from the grid, Fred discharges his battery to the electric utility, making a profit for himself. Now, if Barney observes his own power from the utility, Fred's power to the utility, and the spinning of the windmill. If the windmill is not spinning, information flows from Fred to Barney and Barney can deduce the Fred is not being honest. However, if the windmill is spinning when Barney observes Fred's behavior, he still cannot deduce anything about Fred's behavior. Thus, no information flows from Fred to Barney.

This simple example exhibits the complexities of observation and action of a simple physical system. Smart grid systems couple (intelligent) cyber action with physical operation, dramatically increasing the complexity of determining information flow. This paper examines a future generation smart grid, the *Future Renewable Electric Energy Delivery and Management (FREEDM)* System [15], which is a National Science Foundation(NSF)-funded Energy Research Center (ERC). The FREEDM system is a smart grid managed with a Distributed Grid Intelligence (DGI) to optimize the utilization of renewable energy generation and storage resources, to be integrated with the existing legacy grid. DGI consists of cyber processes that perform distributed computation to efficiently manage physical system resources. As a part of DGI, an application of distributed load balancing to FREEDM, called *Power Balancing* scheme is adopted to perform a power migration among the nodes that are in Supply and Demand of power. FREEDM system contains subtle complexity in its combined information flow

and confidentiality requirements, making it challenging to analyze the system with respect to the known information flow properties. In this paper, we uncover potential confidentiality violations within the system by performing such an analysis.

Several models by which a low-level passive observer may divulge confidentiality within the context of FREEDM have been discussed in this paper. These models differ by the relative setting of the observer and the system; one in which it could be completely external to the system, one in which it is a part of the physical system and one in which it is a part of the combined CPS. A major challenge is to express the physical invariance of power flow and economics in semantics of information flow, so that potential violations of confidentiality due to unrestricted information flow are revealed. This paper treats each of these observer models within this semantic context.

Section 2 introduces some aspects of SPA and BNDC, which are extensively used throughout this paper. Section 3 presents a deeper insight into the FREEDM system and the implementation of the above mentioned distributed power balancing scheme. In Section 4, the proposed approach for the analysis of information flow is discussed. In Section 5, a preliminary investigation on how an active internal observer can manipulate the power balancing scheme for its gains, is presented. Finally, conclusions and future work are presented in Section 6.

2 Background and Related work

2.1 SPA

Security Process Algebra (SPA, for short) [16] [17] is an extension of the Calculus of Communicating Systems (CCS) [18]. The BNF Syntax of SPA to describe the system is [17]: $E ::= 0|\mu.E|E_1 + E_2|E_1|E_2|E\backslash L|E\backslash_I L|E/L|E[f]|Z$
where 0 is the empty process, which cannot do any action; $\mu.E$ can do action μ and then behaves like E; $E_1 + E_2$ can alternatively choose to behave like E_1 or E_2; $E_1|E_2$ is the parallel composition of E_1 and E_2, where the executions of the two systems are interleaved, $E\backslash L$ can execute all the actions E is able to do, provided that they do not belong to $L \cup \bar{L}$ ($\bar{L}$ refer to the output); $E\backslash_I L$ requires that the actions of E do not belong to $L \cap I$; E/L turns all the actions in L into internal τ's; if E can execute action μ, then $E[f]$ performs $f(\mu)$; finally, Z does what E does, if $Z \equiv_{def} E$. Following typical notation, $\tau \in Tr$ are system traces,$\tau\backslash_x$ is a trace purged of all events in the domain of x, $\tau\ |_x$ is a trace restricted to all events in the domain of x, $E_1|E_2$ is the parallel composition of event E_1 and E_2, H, L are High-Level and Low-Level security domains with high-level and low-level user in each domain, and I, O are Inputs and Outputs. The operation $E_1 \underbrace{||}_{A} E_2$ represents the synchronized parallel composition of E_1 and E_2 upon the events from set A.

2.2 Non-inference model

A system is considered secure if and only if for any legal trace of system events, the trace results from the legal trace purged of all High-level events is still a legal trace of the system [4]. Formally, given the set of all possible valid system traces, Tr, the set of low level events, L, and the set of high level events, H, a system is said to be non-inference secure if

$$NI(ES) \equiv \forall \tau \in Tr, (\tau \mid_L \in Tr) \mid_H = \phi \tag{1}$$

In essence this specifies two conditions on the system. First, that for any system trace the restriction of that trace to just the low level events is also a valid system trace. That is just by observing the low level events one can not infer for sure if a high level event occurred.

2.3 Bisimulation-based Non-Deducibility on Composition Model

A system is considered to have the Bisimulation-based Non-Deducibility on Composition (BNDC) property, if it can preserve its security after composition [16] [17] [19]. A system ES is BNDC if for every high-level process Π, a low-level user cannot distinguish ES from $(ES|\Pi)$ (ES composed with any other process Π). In other words, a system ES is BNDC if what a low-level user sees if the system is not modified by composing any high-level process Π with ES. $BNDC(ES) \equiv \forall \pi \in E_H, ES\backslash H \approx_B (ES|\Pi)\backslash H$ where $ES\backslash H$ changes all the H events in ES into internal events. A system is BNDC-preserving if the above property holds for all possible behaviors of the system.

3 FREEDM System Architecture and Power Balancing Scheme

FREEDM, as shown in Figure 2, is envisioned as an architecture for future "Smart Distribution" systems [15] [7]. The FREEDM microgrid is a smart grid with advanced technologies of a Solid State Transformer (SST), Distributed Renewable Energy Resource (DRER), and Distributed Energy Storage Device (DESD) managed with Distributed Grid Intelligence (DGI) to meet the goals of optimal energy management and reliability enhancement. Photo-Voltaic (PV) arrays and Wind turbines are the elements within DRER while DESD consists of high capacity batteries for efficient energy storage. As shown in Figure 3, every residential node, called the Intelligent Energy Management (IEM) node consists of an SST that manages DRER, DESD and a LOAD which is the consumption of power at the household. The DGI is a major cyber aspect in the FREEDM system with each IEM node running a portion of DGI as a process or processes. The DGI process coordinate among themselves through message passing. The IEM nodes control power flow to and from a shared electrical bus, under the direction of cooperating DGI processes.

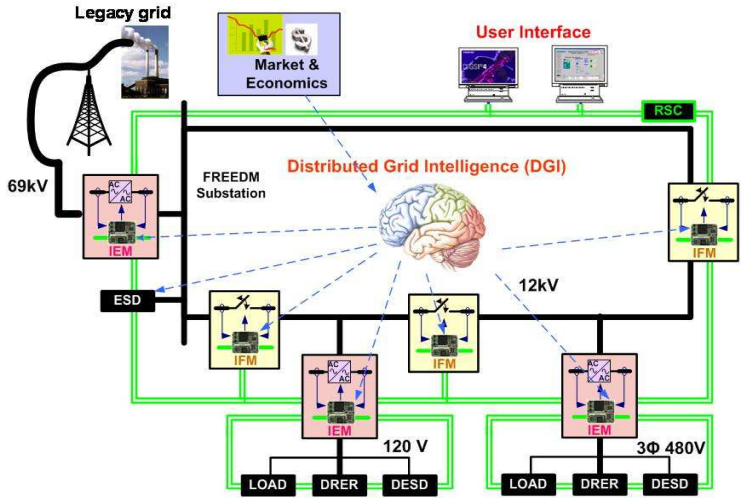

Fig. 2. The FREEDM system overview

3.1 Distributed Power Balancing Scheme

Distributed load balancing algorithms [20] in computer science are designed to normalize the load of process execution among the peers of a distributed system. Intuitively, the nodes participating in a load balancing algorithm communicate their load changes with each other in an attempt to migrate the process execution task from a node with *Demand* to a node with *Supply*. The result of such a migration is that the nodes normalize their loads, thereby achieving a roughly balanced load computation. In this work, one such dynamic process migration scheme [20] is extended beyond its design to a *Power Balancing* scheme that efficiently manages resources in the FREEDM system. Among various algorithms adopted by the DGI is the proposed *Power Balancing* scheme, to efficiently balance power flow through optimal distribution of energy within the system. The implementation of such a Power balancing algorithm in the FREEDM is explained below.

Every IEM computes the SST's actual load on the distribution grid which can be defined as $X_{Actual} = X_{Load}$ - X_{DRER} where, X_{Actual} is the effective load which determines whether the node can *Supply* or it is in *Demand*, X_{Load} is the house load at the SST and X_{DRER} is the power generated by the distributed renewable energy source. The IEM node is in a *Supply* state if $X_{Actual} < 0$, meaning that it has excess generation to *Supply*. It is in a *Demand* state if $X_{Actual} > Threshold$, where $Threshold$ can be decided based on an optimization heuristic. Otherwise, the IEM is in a *Normal* state. The algorithm consists of concurrent sub-processes with message passing communication among the IEMs on critical load changes. Each DGI maintains a (potentially out-of-date) *Load table* as shown in Table 1, to store information it receives about other nodes in the system. Load table updating strategies are adopted to minimize cyber

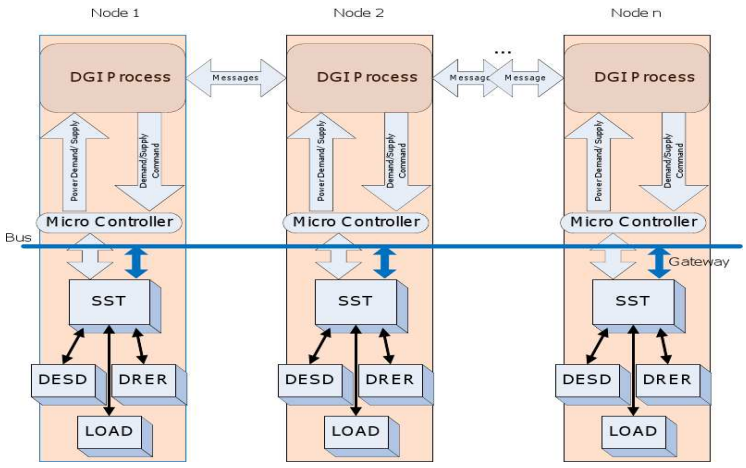

Fig. 3. FREEDM Power Management Architecture

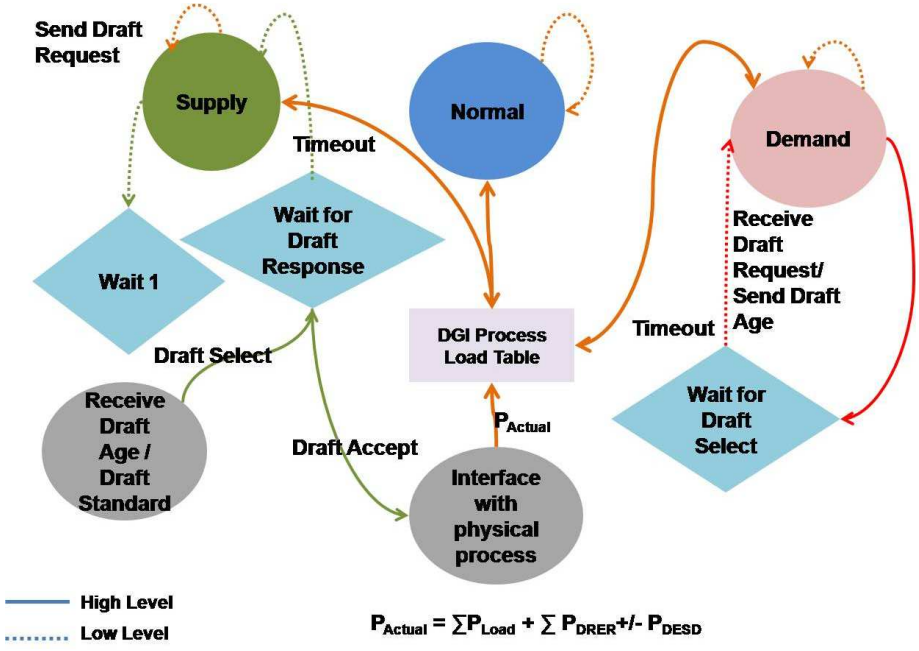

Fig. 4. State diagram of distributed power balancing scheme

message traffic during frequent load changes. As shown in the state diagram of Figure 4, the power balancing process is triggered if at least one node advertises a change of state from *Normal* load level. An IEM node, on entering in to a *Supply* state advertises a *Draft Request* message to the nodes in its load table that are in *Demand* state and waits for response. A *Demand* node, on receiving *Draft Request* message, responds to the sender by sending its demand cost with a special message called *Draft Age*. The *Draft Age* which currently includes the demand to be met by the *Demand* node in order to reach to a *Normal* load level and its corresponding cost are evaluated as in Equation (2).

$$\begin{aligned} Draft\ Age &= X_{Actual} - Threshold \\ Cost_{Demand} &= Draft\ Age * 100 \end{aligned} \tag{2}$$

Node	**State**	**Node**	**State**	. .	**Node**	**State**
1	Supply	1	Supply	. .	1	Normal
2	Demand	2	Demand	. .	2	Demand
.	.	.	.	. .	.	.
.	.	.	.	. .	.	.
n	Supply	n	Supply	. .	n	Normal
At IEM 1		At IEM 2		. .	At IEM n	

Table 1. Load Table maintained at each node

The *Supply* node, on receiving Draft ages from different *Demand* nodes, will compute a *Draft Standard* which is an optimized selection of the node it is going to supply power to by evaluation of factors like its own predicted need, economics and other optimization metrics. It can be observed that the *Draft Age* and *Draft Standard* provide a means to incorporate multi objective function for optimal and economic models of power distribution and management. For simplicity, currently each *Supply* node responds to the request in a First-in First-out (FIFO) order. The *Supply* node, on computation of draft standard, sends a unique *Draft Select* message and initiates the power migration by making a set point on the *Gatewaypower* which is the local SST's individual contribution on to the shared power bus. On receiving the *Draft Select* message from the *Supply* node, the IEM which was in demand receives this power from the shared bus. The migration takes place in unit step size till the time the *Supply* node can supply to the *Demand* node or the *Demand* node meets its sufficient demand, or there is a change of load state in either of the nodes. With every unit of power it receives from the shared power bus (in response to a migration from a *Supply* node), the receiving node would decrement its cost by a factor of 100* *Unit* KW and advertises the updated cost with subsequent migration requests. This multiplication factor of 100 is randomly chosen to prioritize the distribution from DRER generation against the neighboring battery.

$$Cost_{Supply} = 100 * X_{DRER} + X_{DESD} \tag{3}$$

For a *Supply* node, the cost is evaluated as in Equation (3). With every migration step involving *Unit* KW of power, $Cost_{Supply}$ would be decremented by a factor of 100 representing the migration from DRER. Power migration does not take place once this cost is less than the DRER multiplication factor of 100, indicating that the cost remaining is associated with the battery which could be used now on a conditional basis, by querying its *State of Charge*. The algorithm continues till all the nodes are in *Normal* state. SST will automatically consume power from utility to meet inadequate aggregate demand, as long as the utility electric is available with cheaper cost than DESD. A sample DGI trace involving a Drafting node (which can *Supply*) and the source (which is in *Demand*) is shown below:

```
                                        DGI_Draft: Request bid from known
                                                   loaded DGIs
DGI_Source: Respond to bid request      DGI_Draft: Order the response
            if loaded                              messages arbitrarily.
                                        DGI_Draft: Selects power to migrate
                                                   based on cost
DGI_Source: Responds to select message  DGI_Draft: Sends select message
            and commands local SST                 and commands local SST
```

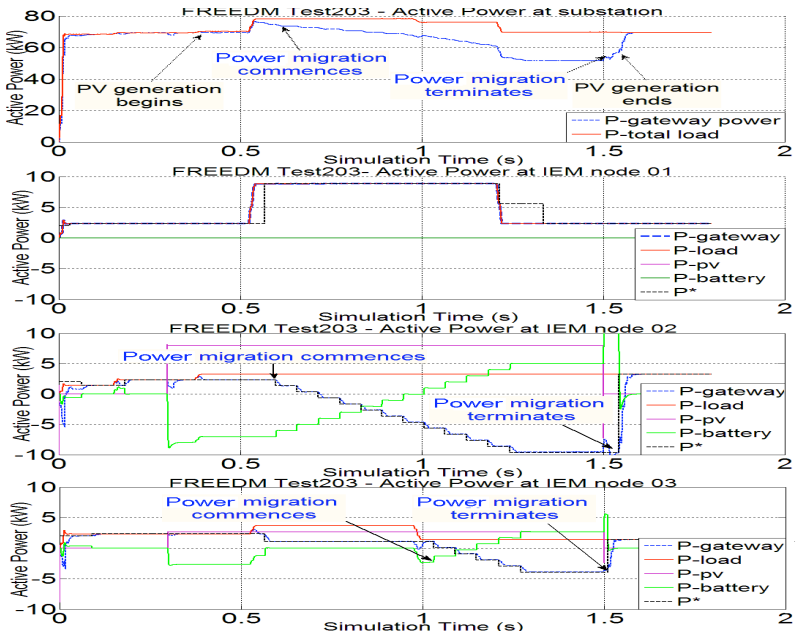

Fig. 5. Power Balancing scheme on 3 IEM nodes

Figure 5 shows the result of power migration with cost bidding, from DRER of three IEM nodes involved in power balancing algorithm. These results were obtained by integrating the DGI process with a *Simulink*© model of the FREEDM system with three IEM nodes. Additional information on this work was described in [21]. It can be observed in Figure 5 that the total active power for the three IEM nodes drops during the period of power migration, indicating the optimality of the algorithm. Initially, IEM node 02 begins migrating power to IEM node 01 which was in a *Demand*. Later at t = 0.9761s, IEM node 03 also reaches to a *Supply* state and then both IEM node 02 and 03 migrate power to IEM node 01 after cost evaluation process.

The implementation of power balancing algorithm for the FREEDM system proved to provide reliable and optimal power distribution and management. Algorithmic properties of load balancing with respect to multi-objective optimization constraints were analyzed in [22]. However, from a security point of view, the effects of power migration at one node can divulge critical information ranging from usage patterns to users observing their Gateway power at other nodes, perhaps violating confidentiality. If a user has access to the state of their DGI, further information can be obtained. Unrestricted information flow can potentially be used against the system for economic gains, under anticipated cap and trade schemes, generators of renewable energy may withhold power to sell at a premium. Such models of information flow are discussed in Section 4.

4 Models of Information Flow

A subnetwork of the FREEDM system with three nodes is depicted in Figure 7. The events in the system are $DRER$, $DESD$, $Load$, Bus, SST and $Utility$ which are the actions associated with DRER, state of DESD, house load, the total power on the shared power bus and strategy of the SST for local management at the node level and utility grid respectively. For notational convenience, the events are distinguished from the actual abbreviations by italicizing them through out the paper. Event classification in to High and Low security levels differ in different scenarios.

Lemma 1. *Power flow in the shared power bus is an invariant function of individual gateway loads of the participating nodes and the draw from or contribution to the utility grid.*

Proof (for lemma). Assuming the utility grid to be an infinite source and sink of power, the power flow in the shared power bus of local grid can be expressed by the Equation 4.

$$P_{Bus} = \sum_{i=1}^{n} P_{Gateway} + P_{Utility} \tag{4}$$

where n is the number of nodes and $P_{Utility}$ is the total power draw from or contribution to the utility grid. This is obvious since the flow in the subnetwork is preserved due to Kirchoff's current laws. The net demand or supply on the bus

is compensated as a net draw from or contribution to the utility grid, respectively. □

Each node without the DGI process can be modeled as in Equation 5.

$$Node_{noDGI} \cong (DRER.\overline{DRER} \sqcap DESD \sqcap Load) \rightarrow X_{SST} \rightarrow (\overline{DESD} \sqcap \overline{Load}).Gateway \rightarrow Node_{noDGI} \quad (5)$$

The invariant on the bus shown in Equation 4 can be modeled as in Equation 6.

$$Bus \cong (Gateway_{Node\ 1}|Gateway_{Node\ 2}....|Gateway_{Node\ n}) \rightarrow Utility \quad (6)$$

The micro grid consisting of n such nodes can be modeled as in Equation 7.

$$E \cong ((Node\ 1_{noDGI}|Node\ 2_{noDGI}|...|Node\ n_{noDGI}) \rightarrow Bus).E \quad (7)$$

4.1 External observer on physical system

The external observer can know visible information about the DRER like size of the facility, weather factors impacting the DRER output (represented by $DRER$), but not the output energy generated at any given instance of time ($\overline{DRER}$). As in Figure 6, the external observer could use electric tools to obtain the reading on the shared power bus or even the gateway at each node since the power lines are physically visible and open. The following conclusions can be made on the information flow in the case of such an observer.

Lemma 2. *A node without DGI is BNDC-secure with respect to a low-level external observer with limited physical observability.*

Proof. Assuming that the low-level observer can only observe the visible DRER sources, the classification of events at any node as defined in Equation 5 is $Low = \{DRER\}$, $High = \overline{DRER}$, $DESD$, $Load$, X_{SST}, $\overline{DESD}$, $\overline{Load}$, $Gateway$. Restricting all the high level events within the node yields, $Node_{noDGI}\backslash H \equiv \{DRER\}$. For any high level process Π, say, $X_{SST}.Gateway$ or $\overline{DRER}.X_{SST}$ the restriction of the composed system, $(Node_{noDGI}|\Pi)\backslash H \equiv \{DRER\}$. Therefore, $E\backslash H \approx_B (E|\Pi)\backslash H$. We can conclude that it cannot distinguish between $Node_{noDGI}$ and $(Node_{noDGI}|\Pi)$ $\forall \Pi \in E$. □

Lemma 3. *A node without DGI is BNDC-secure with respect to a low-level external observer which can read the gateway at the node.*

Proof. Assuming that the low-level observer can observe the visible DRER sources as well as the Gateway, the classification of events at any node as defined in Equation 5 is $Low = \{DRER, Gateway\}$, $High = \{\overline{DRER}, DESD, Load, X_{SST}, \overline{DESD}, \overline{Load}\}$. Restricting all the high level events within the node

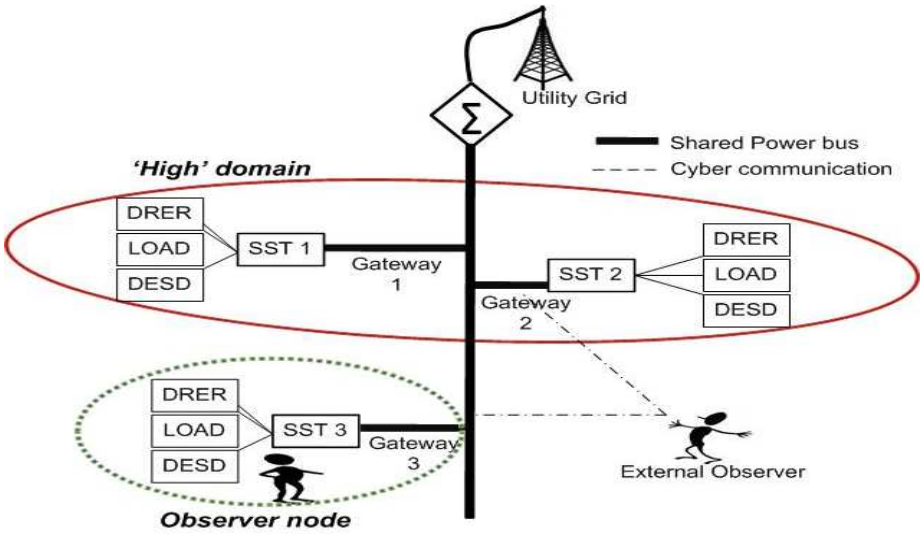

Fig. 6. FREEDM subsystem with no DGI, two nodes and two observers

yields, $Node_{noDGI}\backslash H \equiv \{DRER, Gateway\}$. For any high level process $\Pi \equiv \overline{DRER}.X_{SST}.\overline{DESD}$ or $Load.X_{SST}.\overline{DESD}.\overline{Load}$ the restriction of the composed system, $(Node_{noDGI}|\Pi)\backslash H \equiv \{DRER, Gateway\}$. Therefore, $E\backslash H \approx_B (E|\Pi)\backslash H$. We can conclude that it cannot distinguish between $Node_{noDGI}$ and $(Node_{noDGI}|\Pi)$ $\forall \Pi \in E$. □

Another interesting observation in addition to Lemma 3 is that the process also satisfies non-deducibility property. The observer might see a different output of *Gateway* every time a high level process takes place within the system. However, it cannot deduce anything about the high level inputs to the system since a gateway change might be because of any of the high level inputs $\{\overline{DRER}$, $DESD$, $Load\}$ or a combination of them.

Theorem 1. *The physical system in FREEDM is BNDC-secure with respect to a low-level external observer as shown in Figure 6.*

Proof. From Lemmas 2 and 3, it follows that low-level observations on DRER and gateway at individual nodes is BNDC-secure. When composed with the bus as in Equation 7, the system still satisfies the BNDC property. Assuming that the low-level observer can observe the visible DRER sources as well as the Bus, the classification of events within the system as defined in Equation 7 is $Low = \{DRER^n_{i=1}, Bus\}$, $High = \{Node\ 1_{noDGI}, Node\ 2_{noDGI}$ ... $Node\ n_{noDGI}, Utility\}$. Restricting all the high level events within the system yields, $E\backslash H \equiv \{DRER^n_{i=1}, Bus\}$. For any high level process Π, say, $X^1_{SST}.Gateway\ 1 \rightarrow X^1_{SST}.Gateway\ 2$ the high-level restriction on composed system, $(Node_{noDGI}|\Pi)\backslash H \equiv \{DRER^n_{i=1}, Bus\}$. Due to Lemma 1, observation

of Bus is always consistent since $\sum_{i=1}^{n} Gateway + Utility = \sum_{i=1}^{n} Gateway' + Utility'$. Therefore, $E\backslash H \approx_B (E|\Pi)\backslash H$. □

Given that the observer can observe all the gateway loads, the observer can match every unique $Gateway$ event with a corresponding Bus event, thereby divulging the confidentiality of the system. In that case, restricting all the high level events within the system yields, $E\backslash H \equiv \{DRER_{i=1}^{n}, Gateway_{i=1}^{n}, Bus\}$. For any $\Pi \equiv X_{SST}^{1}.Utility \rightarrow X_{SST}^{2}.Utility$, $(Node_{noDGI}|\Pi)\backslash H \equiv DRER_i$, $Gateway_i'$, $Bus'\}$ where Bus' is inconsistent with the event, Bus. In that case, the system is not BNDC-secure.

4.2 Internal observer on the physical system

If the nodes are not involved in the DGI power balancing process, the low-level internal observer as shown in Figure 6, who is a part of the physical grid can observe a change on the shared power bus, whenever a $Supply$ node renders its excess generation to the utility grid or a $Demand$ node absorbs power from the utility grid. However, the observer cannot exactly tell who performed the change. This leads to the following Lemma 4.

Lemma 4. *The system without the DGI process is non-deducible secure.*

Proof. The change observed by the low level observer on the shared power bus, l_{Bus} could be due to any of the other nodes that are in $Demand$ or $Supply$. The observer would be in doubt as to who performed the event or if more than one of the nodes performed it. The observer could not deduce the high level inputs to the system from the low level observation. This makes the system non-deducible secure. □

Theorem 2. *The physical system in FREEDM is BNDC-secure with respect to a low-level internal observer as shown in Figure 6.*

Proof. Assuming that the low-level internal observer, IO can observe the visible DRER sources as well as the Bus, the classification of events within the system as defined in Equation 7 is $Low = \{DRER_{i=1}^{n}, Node\ IO_{noDGI}, Bus, Utility\}$, $High = \{Node\ 1_{noDGI}, Node\ 2_{noDGI}\ ...\ Node\ n_{noDGI}\}$. Restricting all the high level events within the system yields, $E\backslash H \equiv \{DRER_{i=1}^{n}, Node\ IO_{noDGI}, Bus, Utility\}$. For any high level process Π, say, $X_{SST}^{i}.Gateway\ i \rightarrow X_{SST}^{j}.Gateway\ j$ where $i, j \neq IO$ the high-level restriction on the composed system, $(Node_{noDGI}|\Pi)\backslash H \equiv \{DRER_{i=1}^{n}, Node\ IO_{noDGI}, Bus\}$. As with the case with external observer in Theorem 1, following the Lemma 1, observation of Bus is always consistent since $\sum_{i=1}^{n} Gateway + Utility = \sum_{i=1}^{n} Gateway' + Utility'$. Therefore, $E\backslash H \approx_B (E|\Pi)\backslash H$. □

There could be special cases of the internal observer who can divulge the confidentiality of nodes performing a power migration over the bus. This however, depends on the observer‘s perception of the topology of the system and his

placement. For example, an observer located nearer to the utility grid in a linear network can observe every change on the bus due to the activity of other nodes but cannot exactly infer which of the nodes involved in that event. On the other hand, in a linear network with observer in the middle of the nodes, it can always infer from the changes observed on the bus, the events associated with the its successors in the network tree. Positioning of the observer and number of observation points on such distributed networks to partially deduce the confidential information is discussed in [23].

4.3 Internal observer without DGI, on the physical system composed with DGI

The system composed with power balancing process preserves non-deducibility. Intuitively, this is possible due to the invariance of physical flow as in Equation 4. The nodes participating in power management process make their changes in such a way that the net power flow at the bus remains constant. We have proved this case in our previous work [24] using a gas pipeline system as test case. With Π being the DGI process, LB as defined in Equation 8, each Node can now be defined as in Equation 10.

$$\begin{aligned} LB \cong & (SendDraftRequest \sqcap ReceiveDraftRequest) \rightarrow (ReceiveCost \sqcap \\ & SendCost) \rightarrow (ComputeDraftStandard.DraftSelect \sqcap \\ & AcceptDraft) \rightarrow (Supplier \underbrace{||}_{Migrate} Demander) \end{aligned} \tag{8}$$

$$\begin{aligned} IEM \cong & (DRER.\overline{DRER} \sqcap DESD \sqcap Load) \rightarrow X_{SST} \rightarrow LB \rightarrow \\ & (\overline{DESD} \sqcap \overline{Load}).Gateway \rightarrow IEM \end{aligned} \tag{9}$$

$$E|\Pi = [IEM\ 1|IEM\ 2|..]_n \rightarrow Bus \tag{10}$$

The system composed with the DGI process, $E|\Pi$ can be defined as in Equation 10. Assuming that the low-level internal observer, IO can observe the visible DRER sources, the classification of events within the system as defined in Equation 10 is $Low = \{DRER^n_{i=1}, IEM\ IO, Bus, Utility_{IO}\}$, $High = \{IEM\ 1, IEM\ 2\ ...\ IEM\ n\}$.

Theorem 3. *The system composed with the DGI process, as modeled in Equation 10 satisfies BNDC property with respect to an internal observer without DGI.*

Proof. An internal observer without DGI cannot see the high-level message exchanges associated with the DGI process. Given this, it is unaware of any power migration due to the power balancing algorithm. The high-level restriction of on

the system is $E\backslash H = \{DRER_{i=1}^{n}\} \rightarrow Bus$ and the high-level restriction on the system composed with the DGI, $(E|\Pi)\backslash H = \{DRER_{i=1}^{n}\} \rightarrow Bus'$. However, Bus is consistent with Bus' due to the invariant as defined in Equation 4. The total power on the bus connecting the three nodes as shown in Figure 7to the physical grid is given by $P_{Bus} = P_{Gateway1} + P_{Gateway2} + P_{Gateway3}$. As a result of load balancing, if the migrated power from Node 1 to Node 2 is ζ KW, then $P'_{Bus} = (P_{Gateway1} - \zeta) + (P_{Gateway2} + \zeta) + P_{Gateway3}$. That is, $P_{Bus} = P'_{Bus}$. Also, this event Bus' could also be due to any process, $(X^{i}_{SST}.Gateway.Utility_i) \rightarrow (X^{j}_{SST}.Utility_j)$ where $i, j \neq IO$. Therefore $E\backslash H \approx_B (E|\Pi)\backslash H$, making the system BNDC-secure. □

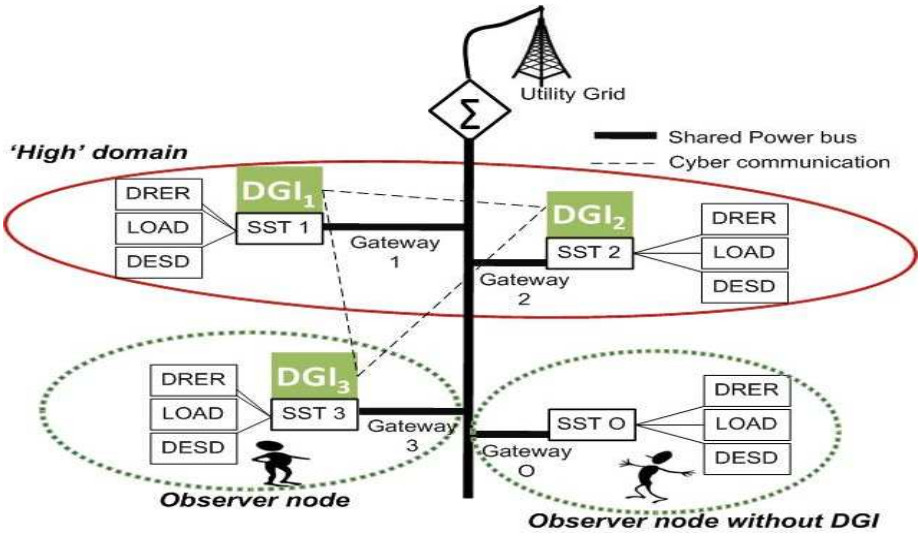

Fig. 7. A FREEDM subsystem with DGI, two nodes and two observers

5 Internal Observer with DGI, on the System Composed with DGI

For an internal observer with DGI as shown in Figure 7, if Node 1 is in Supply state, it could be either supplying to Node 2 or selling power to the utility grid. On the other hand, if Node 2 is in Demand state, it is either receiving power from Node 1 or receiving from utility grid. Such an observer can infer about the global state of the system by the analysis of load table traces that are updated within its DGI process. A load table trace at every node as shown in Table 1, can be represented in the trace model as a sequence of time varying tuples containing the state information. For example, $\Im_{\Delta t} = \{$ (State(Node 1)

at time t1,... State(Node n) at time t1), (State(Node 1) at time t2, .. State(Node n) at time t2), ..}. The observer's view of the system changes depending on the current state of the node, leading to different cases of information flow as below.

5.1 Observer in *Normal* state

Observer can see the nodes that are in *Demand* state from the current trace of its load table, $\Im_{t1}$. However, due to the nature of the distributed algorithm, the nodes marked with state *Supply* and $Normal$ could be out-of-date. This is due to the load table update strategy outlined in Section 3.1. This is good because it makes the system partially BNDC-secure by leaving the observer in doubt about the actual state of the node.

Apart from knowing the state information regarding the *Demand* nodes, the observer could not infer anything about the system. However, by observation of its own load table trace, $\Im$ over a period of time Δt along with the physical observation ($DRER \sqcap Bus$), it can deduce critical information like the $Threshold$ for every node (especially those in *Demand* state) that determines its state, peak utilization and frequency of state change.

Example 1. Consider a system with three IEMs with IEM3 being the low observer, as shown in Figure 7. The load table trace containing the information about the other two IEMs over a period of time Δt is $\Im_{\Delta t} = \{ (Demand, Normal)_{t1}, (Normal, Normal)_{t2}, (Demand, Supply)_{t3}\}$. Assuming that IEM3 is able to estimate P_{DRER} through physical observation, deduces the following information about each node, IEM1 = { t1(Demand, $P_{DRER} = x1$, P_{Load} ¿ y), t2(Normal, $P_{DRER} = x2, y$ ¡ P_{Load}¡= $Threshold_{IEM2}$), t3(Demand, $y3$ ¡ P_{Load}¡ $Threshold_{IEM2}$)} and IEM2 = { t1(Normal, $P_{DRER} = p1$, $q1$ ¡ P_{Load} ¡ $q2$), t2(Normal, $P_{DRER} = p2$, $q3$ ¡ P_{Load}¡ $q4$), t3(Supply, $P_{DRER} = p3$, $y3$ ¡ P_{Load}¡ 0)}. Matching these two traces, IEM3 can deduce that IEM1 transitioned into a $Normal$ state at time t2, because $DESD_{IEM1}$ has discharged and then at time t3, IEM2 was in a *Supply* state; however, since IEM1 which was in demand at that point was not being served by IEM2, IEM3 can deduce that the state information it has about IEM2 is out-of-date. With a large trace set built over a period of time, the information divulged increases, probably leading to a confidentiality violation.

5.2 Observer in *Demand* state

From its Load table trace, observer can see the nodes that are in *Demand* state and *Supply* state. The quantity of information that is observable is more in this case, since it receives the Draft requests from all the nodes that are in *Supply* state. The observer in *Demand* state responds to the draft requests by sending its demand cost (Draft age). If it receives a $Refusal$, it could be because the *Supply* node it responded to has an inadequate matching cost to satisfy its requirement or the *Supply* node has selected to draft with another *Demand* node which has a higher demand cost. In the case with only three IEMs, this doubt

can be resolved as follows: If there is no other *Demand* node that the observer can see, then the *Supply* node does not have enough power to match its requirement. In this case, it can advertise a lesser cost till the time it succeeds. However, at the time it succeeds, it now has an estimate of the excess power the *Supply* node has, with which it can infer its *Load*. Formally, this information flow can be represented as below:

Theorem 4. *The DGI power balancing process is not BNDC-secure with respect to an internal observer in* Demand *state.*

Proof. Let Π be a power balancing process between IEM 1 and IEM 2 as shown in Equation 8. From its load table trace $\Im_t$ ={(Supply, Demand)}, IEM 3 initiates the high-level power balancing process Π' with IEM1. It advertises a cost, $\hat{Cost}_3$ and experiences a refusal, $\mathcal{R}$.

$$IEM\ 1|IEM\ 2 \cong([\Im_t \rightarrow \Pi \rightarrow \hat{Cost}_2]_{IEM1} \underbrace{||}_{Migrate} [\Im_t \rightarrow \Pi \rightarrow \hat{Cost}_2]_{IEM2}) \tag{11}$$

$$(IEM\ 1|IEM\ 2|\Pi') \cong ([\Im_t \rightarrow \Pi \rightarrow \hat{Cost}_2]_{IEM1} \underbrace{||}_{Migrate} [\Im_t \rightarrow \Pi \rightarrow \hat{Cost}_2 \ ]_{IEM2}) \sqcap ([\Im_t \rightarrow \Pi' \rightarrow \hat{Cost}_3]_{IEM1} \underbrace{||}_{Migrate} [\Im_t \rightarrow \Pi' \rightarrow \hat{Cost}_3]_{IEM3})$$

$$(IEM\ 1|IEM\ 2)\backslash H \cong \mathcal{R}$$

$$(IEM\ 1|IEM\ 2|\Pi')\backslash H \cong \Im_t \rightarrow \Pi' \rightarrow \hat{Cost}_3 \rightarrow \mathcal{R}$$

From the above set of equations, obviously $(IEM\ 1|\Pi)\backslash H \not\approx_B (IEM\ 1|\Pi|\Pi')\backslash H$. The proof can easily be extended to n IEMs in the system. Hence the system is not BNDC-secure with respect to an internal observer in *Demand* state.

□

Alternatively, the observer, on experiencing a $Refusal$ of its Draft age, can bid a higher cost till the time it receives a $Draft\ Select$, meaning that it is selected by the *Supply* node to Draft. In this case, cost of the other *Demand* node is divulged, along with interference of high level activity between the *Demand* node and the *Supply* node.

5.3 Observer in *Supply* state

The observer in *Supply* state can have information on the nodes that are in *Demand* state with certainty. It initiates the Draft request to obtain the $Draft\ ages$

from the *Demand* nodes which include their respective demands. It is possible that the *Demand* node experiences a refusal, $\mathcal{R}$ since the observer is not actually ready for migration and the observer can continue this process by which results in the *Demand* node not satisfying its request from any other IEMs in supply state. However, this case can be handled by not accepting any Draft requests from the presumably *Supply* node after a certain number of Refusals. Along with the low level physical observation and these demands advertised by the *Demand* nodes, the observer can infer critical information about DESD, Loads and strategy of SST at the *Demand* node. Formally, it can be represented as in Theorem 5.

Theorem 5. *The DGI process is not BNDC-secure with respect to an internal observer with DGI in* Supply *state.*

Proof. Let Π be a power balancing process between IEM 1 and IEM 2 as shown in Equation 8. Basing on its load table trace $\Im_t$ ={(Supply, Demand)}, IEM 3 initiates the load balancing process Π' with IEM 2. IEM 2 responds with a cost $\hat{Cost}_2$, revealing its demand.

$$IEM\ 1|IEM\ 2 \cong ([\Im_t \rightarrow \Pi \rightarrow \hat{Cost}_2]_{IEM1} \underbrace{||}_{Migrate} [\Im_t \rightarrow \Pi \rightarrow \hat{Cost}_2]_{IEM2}) \tag{12}$$

$$(IEM\ 1|IEM\ 2|\Pi') \cong ([\Im_t \rightarrow \Pi \rightarrow \hat{Cost}_2]_{IEM1} \underbrace{||}_{Migrate} [\Im_t \rightarrow \Pi \rightarrow \hat{Cost}_2]_{IEM2}) \sqcap ([\Im_t \rightarrow \Pi' \rightarrow \hat{Cost}_2]_{IEM3} \underbrace{||}_{Migrate} [\Im_t \rightarrow \Pi' \rightarrow \hat{Cost}_2]_{IEM2})$$

$$(IEM\ 1|IEM\ 2)\backslash H \cong \emptyset$$

$$(IEM\ 1|IEM\ 2|\Pi')\backslash H \cong \Im_t \rightarrow \Pi' \rightarrow \hat{Cost}_2$$

Obviously, $(IEM\ 1|IEM\ 2)\backslash H \ncong (IEM\ 1|IEM\ 2|\Pi')\backslash H$. This proves that the system does not satisfy BNDC property with respect to an internal observer in *Supply* state. The same operation performed by the internal observer (IEM 3 in this case) leads to deducing of critical information regarding IEM 2. The proof can be extended to n nodes in the micro grid. □

6 Conclusions and Future work

The information flow models discussed in Section 4 reveal critical ways in which information can be divulged in the context of FREEDM. The goal of such an analysis is to formally prove how physical observability and the inherent nature

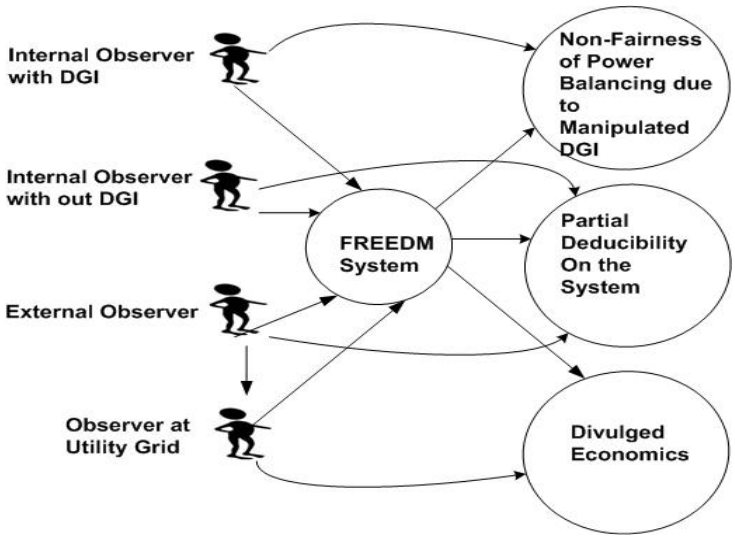

Fig. 8. Usecase scenario for confidentiality violation in FREEDM system

of the cooperating DGI processes lead to partial deducibility of information. The use case diagram presented in Figure 8 depicts how different models of observers could obtain different levels of information. These models present real-time scenarios in which the participants of the system can breach confidentiality with such an information leakage and sometimes, cooperate among themselves to cause unfair energy distribution and non-economic management.

Positioning of the observer, topological considerations and number of observation points to breach the confidentiality within the system are discussed in [23]. The information flow analysis has revealed potential confidentiality violations in the infrastructure considered. A future work is to extend the current information flow analysis by considering models in which the observer can perform physical attacks on the infrastructure and in cases where he can manipulate other DGIs by being an internal part of the system, etc. The FREEDM system design includes the notion of smart loads wherein, the house load can be managed by the DGI process to optimally schedule the component loads. This granularity adds up to the complexity of the existing system in future, leading to a greater confidentiality requirement. Another future work is to generalize this approach to such a complex hierarchical system. The methodology adopted in this paper provides future directions for model-checking Cyber-physical systems for information flow security.

References

1. Goguen, J.A., Meseguer, J.: Security Policies and Security Models. In: Proc. of the IEEE Symposium on Security and Privacy (SSP'82), IEEE Computer Society

Press (2002) 195–204
2. Sutherland, D.: A model of information. In: Proceedings of the 9th National Security Conference. (1986) 175–183
3. McLean, J.: Security models and information flow. In: Procs. of the 1990 IEEE Computer Society Press, IEEE Computer Society Press (1990)
4. McLean, J.: Encyclopedia of Software Engineering - Security Models. (1994)
5. McLean, J.: A general theory of composition for a class of 'possibilistic' security properties. IEEE Transactions on Software Engineering **22**(1) (Jan. 1996) 53–67
6. 110th Congress of United States: Smart grid, Washington DC (2007)
7. Smart Distribution System Design: Automatic Reconfiguration for Improved Reliability. In: IEEE General Meeting, Minneapolis, MN (2010)
8. Laurence Phillips, Hamilton Link, R.S., Welland, L.: Agent-based control of distributed infrastructure resources. Technical report, Sandia National Laboratories, Albuquerque, New Mexico (2006) SAND2005-7937.
9. IEEE: (IEEE P1547.4 Draft Guide for Design, Operation, and Integration of Distributed Resource Island Systems with Electric Power Systems)
10. Matti Lehtonen, Anssi Seppala, V.K.P.K.G.K., Lemstrom, B.: Distribution energy management in the environment of de-regulated electricity market. In: Proc. Energy Management and Power Delivery. Volume 2. (1995) 516–521
11. Nikkhajoei, H., Lasseter, R.H.: Microgrid protection, Proc. IEEE Power Engineering Society General Meeting (2007) 1–6
12. Lasseter, R.H.: Dynamic distribution using (der) distributed energy resources. In: Proc. IEEE Power Engineering Society Transmission and Distribution Conference and Exhibition. (2006) 932–934
13. McDaniel, P., McLaughlin, S.: Security and privacy challenges in the smart grid. Security Privacy, IEEE **7**(3) (2009) 75 –77
14. Chronicles, M.R.: What will talking power meters say about you? http://redtape.msnbc.com/2009/10/would-you-sign-up-for-a-discount-with-your-power-company-in-exchange-for-surrendering-control-of-your-thermostat-what-if-it.html (2009) [Online; accessed 19-March-2010].
15. Huang, A.: Renewable energy system research and education at the NSF FREEDM systems center. In: Power & Energy Society General Meeting, 2009. PES '09. IEEE. (2009) 1–6
16. Focardi, R., et al.: The compositional security checker: A tool for the verification of information flow security properties. IEEE Transactions on Software Engineering **23**(9) (Sept. 1997)
17. Focardi, R., Gorrieri, R.: A classification of security properties for process algebras. Computer Security **3**(1) (1994/1995) 5–33
18. Milner, R.: Communication and Concurrency. Prentice Hall (1989)
19. Focardi, R., Gorrieri, R., , Martinelli, F.: Real-time information flow analysis. IEEE Journal on Selected Areas in Communications **21**(1) (Jan. 2003)
20. Ni, L.M., Xu, C.W., Gendreau, T.B.: A distributed drafting algorithm for load balancing. IEEE Trans. Softw. Eng. **11**(10) (1985) 1153–1161
21. Ravi Akella, Fanjun Meng, Derek Ditch, Bruce McMillin and Mariesa Crow: Distributed Power Balancing for FREEDM system. Technical report, Missouri University of Science and Technology, Rolla, MO, USA (2010) Available at http://filpower.mst.edu/documents/Akella-FreedmAC10.pdf.
22. Ditch, D., McMillin, B.: An application of load balancing for optimal power distribution. Technical report, Missouri University of Science and Technology, Rolla, MO, USA (2010) Available at http://filpower.mst.edu/documents/Ditch-FreedmAC10.pdf.

23. Ditch, D.P., McMillin, B.M.: The security implication of multiple observers in a distributed system. Computer Software and Applications Conference, Annual International **2** (2009) 341–346
24. Akella, R., McMillin, B.M.: Model-Checking BNDC Properties in Cyber-Physical Systems. Computer Software and Applications Conference, Annual International **1** (2009) 660–663