



# Physical Attestation of Cyber Processes in the Smart Grid

Tom Roth, Ph.D. Student ([tprfh7@mst.edu](mailto:tprfh7@mst.edu))  
 Bruce McMillin, Ph.D. ([ff@mst.edu](mailto:ff@mst.edu))

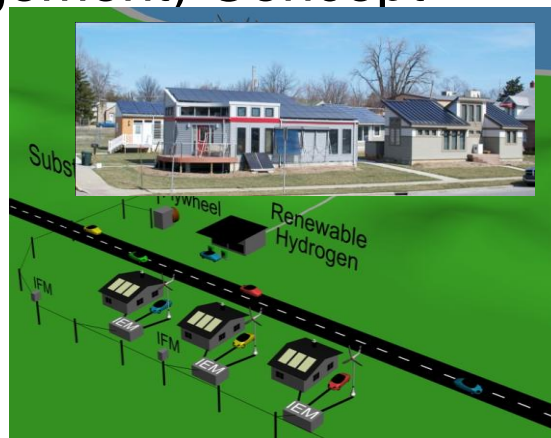
Department of Computer Science  
 Missouri University of Science and Technology  
 (Formerly the University of Missouri-Rolla)  
 Rolla, MO 65409-0350

Supported in part by the Future Renewable Electric Energy Delivery and Management Systems Center (FREEDM) under grant NSF EEC-0812121 and in part by the Missouri S&T Intelligent Systems Center.

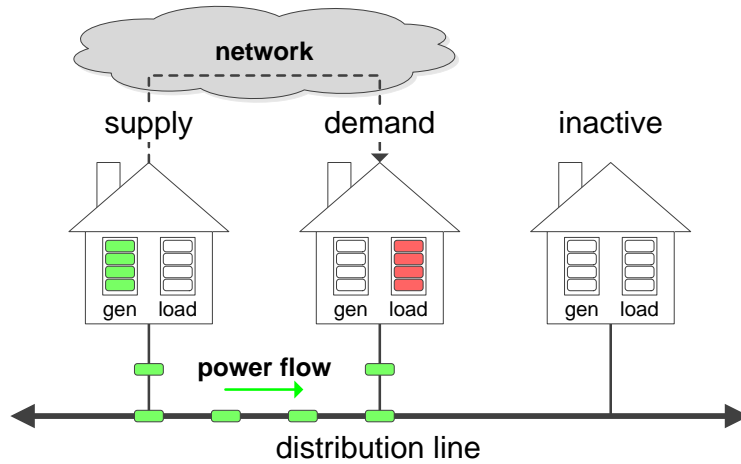


## The FREEDM (Future Renewable Electric Energy Delivery and Management) Concept

- Distributed Grid Intelligence (DGI)
  - People share energy resources
  - Neighborhood or industrial level
  - Where is the centralized controller?
  - Peer-to-peer

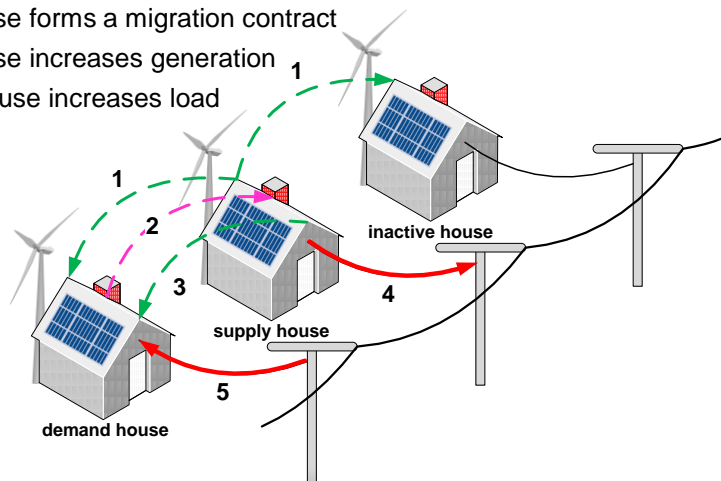


# Smart Neighborhood



## Power Migrations

1. Supply house advertises its excess generation
2. Demand house requests power from supplier
3. Supply house forms a migration contract
4. Supply house increases generation
5. Demand house increases load



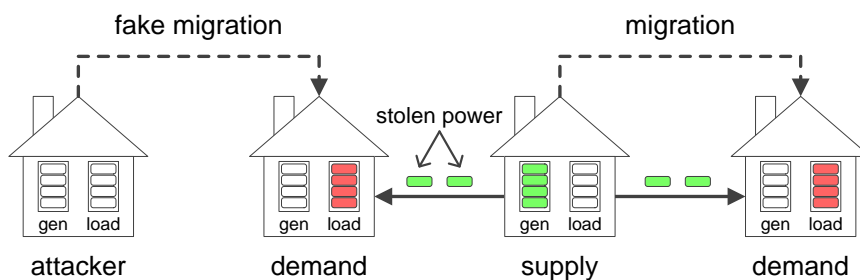
## New Threats - Distributed System

- The current electric power grid relies on the notion of a centralized power authority.
- No centralized authority is involved with the distributed process of power migrations.
- A compromised house can trick its peers into making bad power migrations in the absence of the centralized authority.

## Fake Supply Attack

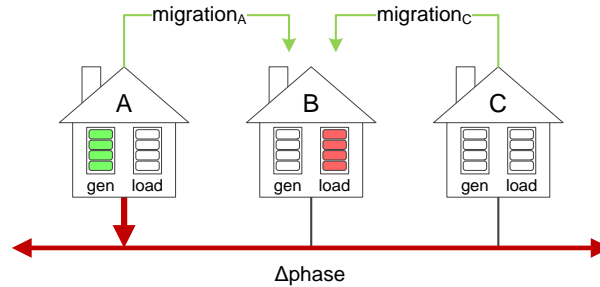
Consider an attack that removes one step from the system operation:

1. Supply house advertises its excess generation
2. Demand house requests power from supplier
3. Supply house forms a migration contract
- ~~4. Supply house increases generation~~
5. Demand house increases load



# Concurrent Fake Supply Attack

- House C launches a fake supply attack during a migration from A:



- During the attack, the low-level view of house B is:



- This view is consistent with either  $increase_A$  or  $increase_C$ !

## Information Flow Models

### – Non-Interference

- High-level events do not interfere with the low level outputs

### – Non-Inference

- Removing high-level events leaves a valid system trace

### – Non-Deducibility

- Low-level observation is compatible with any of the high-level inputs.

Typically we use these to blind an attacker, here we use them to model a STUXNET-like attack

# Nondeducible Attack

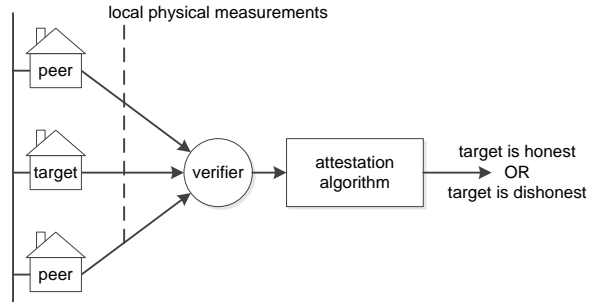
- Definition:  
A low-level view of a system is *nondeducible* if the view is consistent with all permutations of high-level commands.
- Theorem:  
An attacker who launches a fake supply attack concurrent with another migration in the system is *nondeducible* and thus unidentifiable.

# Solutions in Literature

- **Tamper Resistance:**  
Prevent an attack using compromise-resistant hardware.
- **Bad Data Detection:**  
Detect malicious meter readings at a centralized controller.
- **Distributed Diagnosis:**  
Detect a fault using peer evaluations in a distributed system.
- **Remote Attestation:**  
Detect a compromised node using a challenge-response protocol.

# Physical Attestation

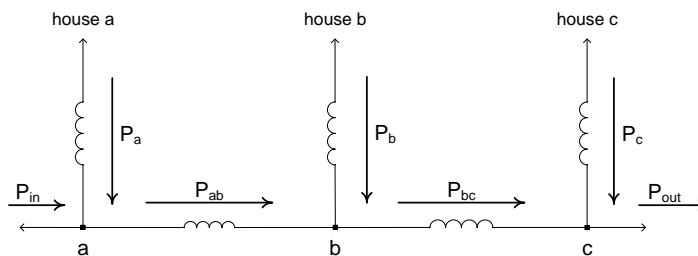
- A verifier checks if another cyber process is compromised using physical measurements.



- Similar to a remote attestation algorithm that uses the physical layer as a shared memory.

# Conservation of Power

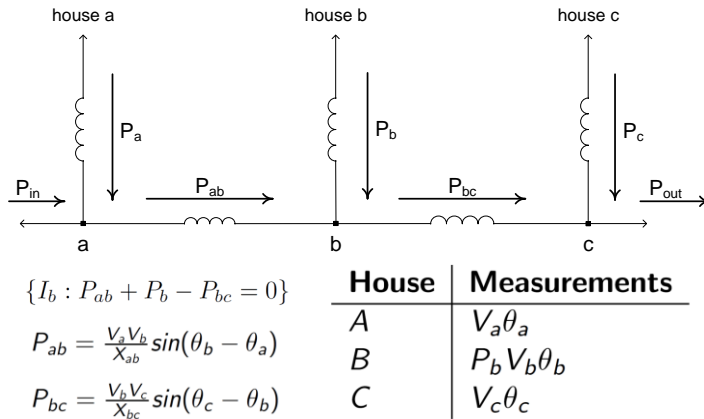
- Conservation of Power at  $b$ :  $\{I_b : P_{ab} + P_b - P_{bc} = 0\}$



- $I_b$  is an invariant that must be true for the physical system.
- If  $I_b$  is violated, then at least one house must be dishonest.

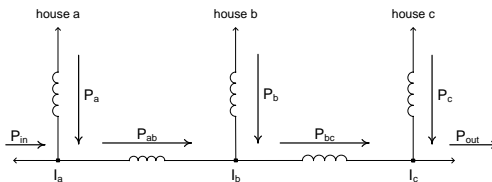
# Physical Measurements

- The invariant is instantiated using measurements from each house:



## Impact of Compromised Node

- Assume  $b$  is malicious and the other two houses are honest.



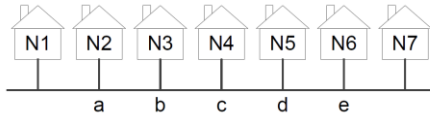
- A set of invariants are violated when  $b$  falsifies its values:

Falsified Values	Violated Invariants
$P_b$	$I_b$
$V_b \theta_b$	$I_a I_b I_c$
$P_b V_b \theta_b$	$I_a I_c$

- The dishonest house is the midpoint of each violation set.

# Unique Violation Pattern

- It requires observations from 7-houses to find a unique violation pattern:



- It is not possible to produce a unique pattern with fewer observations.
- This set of observations can be used to detect when house 4 performs a fake supply attack

N	Falsified	Violations
1	$V_1\theta_1$	$l_a$
2	$P_2$ $V_2\theta_2$ $P_2V_2\theta_2$	$l_a$ $l_a l_b$ $l_b$
3	$P_3$ $V_3\theta_3$ $P_3V_3\theta_3$	$l_b$ $l_a l_b l_c$ $l_a l_c$
4	$P_4$ $V_4\theta_4$ $P_4V_4\theta_4$	$l_c$ $l_b l_c l_d$ $l_b l_d$
5	$P_5$ $V_5\theta_5$ $P_5V_5\theta_5$	$l_d$ $l_c l_d l_e$ $l_c l_e$
6	$P_6$ $V_6\theta_6$ $P_6V_6\theta_6$	$l_e$ $l_d l_e$ $l_d$
7	$V_7\theta_7$	$l_e$

# Attestation Algorithm

## Algorithm 1: Secure Power Calculation

---

Data: Index  $t$  of the node to attest  
 Data: The *time* of the attestation  
 Data: A small tolerance  $\epsilon$   
 Result: Actual generation  $P_t$  at node  $t$

```

1 get values  $\{\hat{P}_{t-2}, \dots, \hat{P}_{t+2}\}$  for given time // get cyber message history
2 get values  $\{V_{t-3}\theta_{t-3}, \dots, V_{t+3}\theta_{t+3}\}$  for given time // get physical meter readings
3 for  $i \leftarrow t-2$  to  $t+2$  do // evaluate each invariant
4    $P_{i-1,i} \leftarrow \frac{V_{i-1}V_i}{X_{i-1,i}} \sin(\theta_i - \theta_{i-1})$ 
5    $P_{i,i+1} \leftarrow \frac{V_iV_{i+1}}{X_{i,i+1}} \sin(\theta_{i+1} - \theta_i)$ 
6   if  $|P_{i-1,i} + \hat{P}_i - P_{i,i+1}| < \epsilon$  then
7      $l_i \leftarrow \text{true}$ 
8   else
9      $l_i \leftarrow \text{false}$ 
10 if  $\neg l_{t-1}$  and  $\neg l_{t+1}$  OR  $\neg l_t$  and  $(\forall k \neq t)(l_k)$  then // check the violation pattern
11    $P_{t-1,t} \leftarrow P_{t-2,t-1} + \hat{P}_{t-1}$ 
12    $P_{t,t+1} \leftarrow P_{t+1,t+2} - \hat{P}_{t+1}$ 
13   return  $P_{t,t+1} - P_{t-1,t}$  // case when  $t$  is dishonest
14 else
15   return  $\hat{P}_t$  // case when  $t$  is honest

```

---



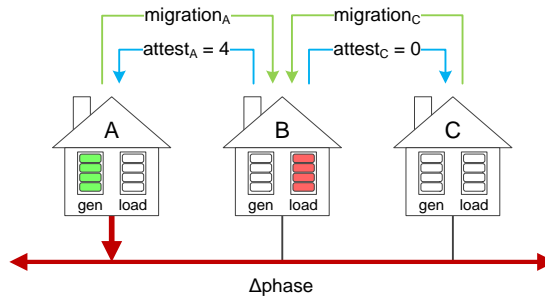
# System Modifications

Two modifications make the fake supply attack deducible:

1. Supply house advertises its excess generation
2. Demand house requests power from supplier
3. Supply house forms a migration contract
4. Supply house increases generation
- 5. Demand house performs attestation as a verifier**
- 6. If attestation passes, demand house increases load**

## Deducible Fake Supply Attack

- House C launches a fake supply attack during a migration from A:



- During the attack, the low-level view of house B is:



- This view is **not** consistent with  $increase_C$  and therefore deducible!

## Conclusion

- A software solution to compromised peers that mitigates the need for new hardware.
- More powerful than remote attestation since an attacker cannot hide the effect of its actions on the physical layer.
- Current algorithm is limited to one attack type on linear physical topologies.
- Shows new kinds of vulnerabilities induced by peer-to-peer energy and power management

<http://freedm.ncsu.edu>

**FREEDM**  
systems center

About News, Events, & Media ATEC Research Education Industry Join

**About :: Center Goals**

The goal of NSF's Gen-III ERC Program is to create a culture of innovation in engineering research and education that links scientific discovery to technological innovation through transformational engineered systems research. ERC's make advances in technology and produce engineering graduates who will be creative innovators in a global economy.

Specifically, the FREEDM Systems Center's goals are:

- Develop the fundamental knowledge base for the FREEDM system and provide fundamental breakthrough technology in energy storage and power semiconductor devices
- Develop enabling technologies for subsystem and system demonstrations
- Develop a one-megawatt FREEDM green energy hub system to power the ERC headquarters and other buildings on NC State's Centennial Campus
- Form long-term partnerships with large and small firms to speed the translation of ERC research into commercially viable products, stimulate formation of start-up companies based on ERC intellectual property, and involve students in all phases of the innovation process
- Develop a diverse group of adaptive, creative, and innovative graduates who advance fundamental knowledge, enabling technology and engineered systems innovations in renewable electric energy delivery and management systems
- Develop long-term partnerships with middle and high schools, teachers, and students to enhance engineering content knowledge and pedagogical methods, bring engineering concepts into the classroom, involve pre-college students in research, and increase the diversity and enrollment of domestic students in university engineering degree programs
- Increase the diversity of the proposed Center's leadership, faculty, and students to exceed academic engineering nationwide averages within the first five years of operation.

NC STATE UNIVERSITY FLORIDA A&M UNIVERSITY FLORIDA STATE UNIVERSITY MISSOURI S&T ASU RWTH AACHEN UNIVERSITY ETH