Security and Privacy Issues In Smart Grid

J. Liu and Y. Xiao, S. Li, W. Liang, C. Chen
IEEE COMMUNICATIONS SURVEYS & TUTORIALS, to appear

Wednesday, September 26, 2012

Mohamed M. E. A. Mahmoud

PhD, PDF, and Visiting Professor, University of Waterloo, Ontario, Canada
Postdoctoral Fellow, University of Ryerson, Toronto, Ontario, Canada

http://bbcr.uwaterloo.ca/~mmabdels/   mmabdels@bbcr.uwaterloo.ca
Outline

- What is Smart Grid? Applications and Benefits
- Security Issues
- Privacy Issues
- Future Research Directions
The smart grid is a promising power delivery infrastructure that integrates information technology, digital communications, sensing, measurement and control technologies into the power system.

Through advanced sensing technologies and control methods, it can capture and analyze data regarding power usage, delivery, and generation in near real-time.

Objective: to evolve the architecture into a more distributed, dynamic system characterized by **two-way flow of power and information**.
According to the analysis results, the smart grid may provide **predictive information** and **corresponding recommendations** to all stakeholders (e.g., utilities, suppliers, and consumers) regarding the optimization of their power utilization.

It may also offer services like intelligent appliance control for energy efficiency and better integration of distributed energy resources (DERs) to reduce carbon emissions.

It is not a simple grid - it can be regarded as a “**system of systems**”.

Such a complex system undoubtedly presents many challenges, especially in cyber security and privacy aspects.
The unique characteristics of smart grid comparing to IT networks

Why new protocols/schemes are needed?

<table>
<thead>
<tr>
<th>Categories</th>
<th>IT Networks</th>
<th>Smart Grid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Objectives</td>
<td>Confidentiality &gt; Integrity &gt; Availability</td>
<td>Availability &gt; Integrity &gt; Confidentiality [3]</td>
</tr>
<tr>
<td>Architecture</td>
<td>1) flexible and dynamic topology; 2) center server requires more protection than periphery hosts [30].</td>
<td>1) relatively stable tree-like hierarchy topology; 2) some field devices require the same security level as the central server [30].</td>
</tr>
<tr>
<td>Technology</td>
<td>1) diverse operating systems; 2) public networks; 3) IP-based communication protocols</td>
<td>1) proprietary operating systems; 2) private networks; 3) IEC61850- and DNP (Distributed Network Protocol) -based communication protocols</td>
</tr>
<tr>
<td>Quality of Service</td>
<td>1) transmission delay and occasional failures are tolerated; 2) allow re- booting [30].</td>
<td>1) high restrictions on transmission delay and failures; 2) rebooting is not acceptable [30].</td>
</tr>
</tbody>
</table>
The U.S. Department of Energy (DOE) stated the design features and benefits for smart grid as follows:

1) **Enabling Informed Participation by Customers:**

   Unlike traditional power systems, customers are better informed by a two-way communication technology.

   The entire smart grid becomes an active electricity market that allows customers to **shift load** and **to generate and store energy** based on near real-time prices.

   Through bidirectional electricity flow, customers are also able to sell stored energy back to the grid when the price is high.

   Such demand-response mechanisms help the grid balance power supply and demand, thus enhancing the efficiency of power usage.

2) **Accommodating All Generation and Storage Options:**

   The smart grid not only accommodates remote centralized power generation, but **also adopts diverse and widespread distributed energy resource** (DER) (e.g., solar, wind, or geothermal energy).

   This concept is proposed to alleviate peak load, to support back-up energy during emergencies.
3) **Enabling New Products, Services, and Markets:**

By using consumer-oriented “smart appliances” or intelligent electronic devices (IEDs), customers or authorized service providers can remotely control IEDs’ power usage.

4) **Providing the Power Quality for the Range of Needs:**

Power quality involves factors like voltage flicker, voltage volume, momentary interruptions, etc.

Different consumers may have distinct power quality requirements (e.g., industrial vs. residential users).

To satisfy a particular consumer’s power usage, the smart grid must meet a wide range of power quality needs.
5) Optimizing Asset Utilization and Operating Efficiently:

The smart grid manages a variety of appliances, facilities, and DERs. Optimizing the utilization of those assets and enabling efficient operation and maintenance will **reduce investment costs**.

6) Operating Resiliently to Disturbances, Attacks, and Natural Disasters:

This concept is proposed to ensure the reliability of the power grid. Regardless of the type of physical damages, the smart grid can effectively resist these problematic events through local, regional, and national coordination.

Authorized operators can quickly isolate the suspected grid components and readjust nearby DERs to support the affected areas. ("**self-healing**")
Fig. 1. NIST reference model for the smart grid [4]
Each one of (Bulk Generation, Transmission, Distribution, and Customers) can generate, store, and deliver electricity in two-way.

(Markets, Service Providers, and Operations) mainly manage the movement of electricity and provide relevant information or services to power consumers and utilities.

**Three types of customers are present in this model:**

HAN (Home Area Network), BAN (Building Area Network), and IAN (Industrial Area Network).

Within those areas, AMI (Advanced Metering Infrastructure) is deployed to monitor all incoming and outgoing electrical and communication flow.
1) **AMI (Advanced Metering Infrastructure):**

*AMI is* an integration of multiple technologies that provides intelligent connections between consumers and system operators.

It is designed to help consumers know the near-real-time price of electricity and thus to optimize their power usage accordingly.

It also helps the grid obtain valuable information about consumers’ power consumption in order to ensure the reliability of the electrical power system.
2) **SCADA (Supervisory Control and Data Acquisition):**

SCADA system is responsible for the real-time monitoring and control of the power delivery network.

3) **PHEV (Plug-in Hybrid Electric Vehicle)**

PHEVs, could also provide a means to support distributed energy resources.

Parked PHEVs can supply electric power to the grid.

This vehicle-to-grid concept may improve the efficiency and increase the reliability of the power grid.

4) **Communication Protocols and Standards**

Protocols for SCADA communication systems

Since the interval of transmitting messages over SCADA networks is limited to 4 milliseconds (according to the IEC 61850-8-1), general encryption or other security methods are not feasible.
Outline

- What is Smart Grid? Applications and Benefits
- **Security Issues**
- Privacy Issues
- Future Research Directions
1) Device Issues

2) Networking Issues

3) Management Issue

4) Anomaly Detection Issues

5) Other Issues

1) Device Issues

Devices are widely deployed in smart grid. This also enables malicious users to manipulate the device and disrupt normal operations of the grid, such as:

- **Shutting down devices to disconnect power services**
- **Tampering with sensing data to misguide the decisions of the operators.**
- **Switching-off hundreds of millions of smart meters with remote off switches.**

- Addressing this problem may require hardware support (tamper proof devices).

For embedded systems, possible approaches for securing software development and upgrade:

1- issue a public key to each device and encrypt all new software with the corresponding private key. The device can then validate the source of the updated patch.

2- “high assurance boot” (HAB) method. The embedded system will be validated once it boots up. The validation script is safely coded into its hardware by the manufacturer.
Tens of millions of sensors are deployed in the grid. These devices have limited bandwidth, power (battery or long sleep cycles), storage, memory, and intermittent connections. Because of these constraints, key management should require less centralization and more persistent connectivity than current approaches.

NIST requirements [3] suggest that each device has unique key and credential materials such that, if one has been compromised, others will not be affected.

<table>
<thead>
<tr>
<th>Topics</th>
<th>Cyber Security Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Key Words</td>
</tr>
<tr>
<td>Smart Meter</td>
<td>• Customer tariff varies on individuals, and thus, breaches of the metering database may lead to alternate bills [3]</td>
</tr>
<tr>
<td>Customer Interface</td>
<td>• Home appliances can interact with service providers or other AMI devices. Once manipulated by malicious intruders, they could be unsafe factors in residential areas [3], [14]. • Energy-related information can be revealed on IEDs or on the Internet. Unwarranted data may misguide users’ decisions [3].</td>
</tr>
<tr>
<td>PHEV</td>
<td>• PHEV can be charged at different locations. Inaccurate billing or unwarranted service will disrupt operations of the market [3].</td>
</tr>
</tbody>
</table>
## 1) Networking Issues

<table>
<thead>
<tr>
<th>Topics</th>
<th>Cyber Security Issues</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internet</strong></td>
<td>- Certain applications may be built on the Internet. Inherent problems like malicious malware and denial of service (DoS) attacks are threats to the grid operations [1], [3], [17], [30], [32].</td>
<td>- Adopt TCP/IP for smart grid networks [1], [3]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- VPN (IPSec), SSH, SSL/TLS [17], [40], [67]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Intrusion detection and firewalls 17,30.</td>
</tr>
<tr>
<td><strong>Networking</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Wireless Network</strong></td>
<td>- In wireless networks, layer 2/3 can be easily attacked by traffic injection and modification. Without routing security, traffic on these layers is not reliable [3], [17].</td>
<td>- Protect routing protocols in layer 2/3 networks [3]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security capabilities in 802.11i, 802.16e, and 3GPP LTE [27]</td>
</tr>
<tr>
<td><strong>Sensor Network</strong></td>
<td>- Sensor data is critical for the grid. Intercepting, tampering, misrepresenting, or forging these data will damage the grid [3], [30].</td>
<td>- AES (Advanced Encryption Standard) encryption [31], [61]</td>
</tr>
</tbody>
</table>
3- Management Issue

Smart grid can be regarded as a combination of several micro grids.

Each micro grid operates autonomously within its local SCADA system and interacts with others.

All micro grids will be controlled by a central master SCADA system.

Those SCADA systems are isolated and controlled by authorized personnel. The system can be compromised as follows:
1) Taking down the SCADA server by the traditional denial of service attacks
2) Gaining control over the system by planting a Trojan into the system
3) Stealing data from the database, e.g., access to the system passwords and usernames.
4) The intruders might be able to access the billing information. There needs to be a powerful firewall to protect the servers from losing this information.
7) Misuse the SCADA servers to attack the other servers in the system and gain access information to the valuable information from the utility companies.

Smart meters may report incorrect data to let the grid makes wrong decisions

Data encryption and digital signatures are required to secure communications. Most of existing cryptographic scheme lack of efficiency under limited space and computation.
Anomaly Detection Issues

Reliable operations of the smart grid require accurate and timely detection for anomalous events.

Intrusion detection System: identifying deviations from a correct behavior.

<table>
<thead>
<tr>
<th>Topics</th>
<th>Cyber Security Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Key Words</strong></td>
</tr>
<tr>
<td>Anomaly Detection</td>
<td><strong>Potential Problems</strong></td>
</tr>
<tr>
<td>Temporal Information</td>
<td>• Unsecured time information may be used for replay attacks and revoked access, which has a significant impact on many security protocols [3], [36].</td>
</tr>
<tr>
<td></td>
<td>• Timestamps in event logs may be tampered by malicious people. [3].</td>
</tr>
<tr>
<td>Data &amp; Service</td>
<td>• RTUs may be damaged in various ways. The accuracy of transmitted data and the quality of services therefore can not be guaranteed [33].</td>
</tr>
<tr>
<td></td>
<td>• Use phasor measurement units (PMUs) to ensure accurate time information [3].</td>
</tr>
<tr>
<td></td>
<td>• Adopt existing forensic technologies to ensure temporal logs are accurate [3].</td>
</tr>
<tr>
<td></td>
<td>• Utilize fraud detection algorithms and models used in credit card transaction monitoring [3].</td>
</tr>
</tbody>
</table>
### Other Issues

<table>
<thead>
<tr>
<th>Topics</th>
<th>Cyber Security Issues</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Words</strong></td>
<td>Potential Problems</td>
<td></td>
</tr>
</tbody>
</table>
| Demand Response | - Tampering with information of real time pricing (RTP) may cause financial and legal problems [3], [25], [30], [59].  
- Malware may infect the grid, indicating false trend of supply and demand. This causes substantial damage to the power delivery system [27], [32], [48]. | - Deploying trusted computing platforms [27]. |
| Others          |                                             |                                     |
| Protocols & Standards | - Existing protocols may have some inherent security flaws [30], [32]. | - More secure standards for automation and communication must be developed [29]. |

The adverse effects could include sending misleading data to the field device or control center operator resulting in

1) Financial loss if the attack leads to excess generation output;

2) Physical danger if a line is energized while linemen are in the field servicing the line;

3) Equipment damage if control commands sent to the field result in overload conditions.
Security requirements

1- User Authentication
Ability to make sure of the identity of the parties sending data

2- Non-Repudiation
Ability to prevent an authorized party from denying the existence or contents of a communication session

3- Access control
Unauthorized user should not access the system
4- Availability

Attackers may exploit flaws in the system to sabotage the grid.
6- Data Integrity

Ability to make sure that information has not been subject to additions, deletions, or modifications.

The aim is to steal service, report wrong generated electricity data for collecting money, or report incorrect information to affect the grid stability.

References:
Outline

- What is Smart Grid? Applications and Benefits
- Security Issues
- Privacy Issues
- Future Research Directions
Smart meters provide near real-time information about electricity usage. Unprotected customers’ electricity consumption data will cause invasions of privacy in the smart grid.

In particular, it may disclose information about:

Where people were and when and what they were doing.

When the home is occupied and it is unoccupied, when occupants are awake and when they are asleep, how many various appliances are used, etc.

**Graph:**
- Peak = 7.18 kW
- Mean = 0.49 kW
- Daily load factor = 0.07 kW
- Energy consumption = 11.8 kWh

- Hob heaters
- Oven preheating
- Oven cycling
- Toaster
- Kettle
- Washing machine
- Refrigerator

**Time of day, h:**
- 00:00
- 02:00
- 04:00
- 06:00
- 08:00
- 10:00
- 12:00
- 14:00
- 16:00
- 18:00
- 20:00
- 22:00
- 00:00
Failure to address privacy issues in the smart grid will not be accepted by customers.

**Smart meters debate in B.C.**

- BC Hydro is replacing analog meters with smart meters, which are capable of providing hourly information about electricity consumption.
- But, more than 15,000 residents signed petitions opposing the devices.
- **Privacy concerns**
  Smart meters invade their privacy by documenting hour-by-hour use of electricity.


**In the news today:**

Ottawa police officer demoted for using database to snoop on ex-lover

Privacy is a very big deal
Who attacks the system usually the people who access it.
Outline

- What is Smart Grid? Applications and Benefits
- Security Issues
- Privacy Issues
- Future Research Directions
Three areas should be further studied to enhance the security level of the grid:

1) integrity and confidentiality of the transmitted data,
2) building a robust and efficient management model for SCADA system,
3) establishing a universal policy and standard for secure communication.

Possible future research directions may include:

**1- Control System Security**

**2- Accountability**

Although security technologies may well protect the grid, new vulnerabilities and risks continue to emerge.

As a complement to security technologies, accountability is required to further secure the smart grid.

Accountability mechanism will determine **who is responsible for a security breach**.

no one can deny their actions, not even the administrators or other users.
3- **Integrity and Confidentiality**
Integrity and confidentiality are two main aspects for computer and network security design.

For example, integrating with huge numbers of DERs may incorporate with distributed database management system and cloud computing technologies.

4- **Privacy**
Privacy issues may be addressed by adopting newly anonymous communication technologies.

Current approaches to anonymize traffic in general networks will cause overhead problems or delay issues.

For some time-critical operations, limited bandwidth and less connectivity features in the smart grid may hinder the implementation of anonymity.
Thank You!

Mohamed M. E. A. Mahmoud