Secure Networked Control Systems Against Replay Attacks Without Injecting Authentication Noise

Luis Alvergue, Bixiang Tang, and Guoxiang Gu
School of Electrical Engineering and Computer Science
Louisiana State University

September 19, 2014
Outline

Smart Grid

Smart Grid Security

Conclusion

References

Questions
Smart Grid

Modern Power Grids

- Distributed generation units and loads contribute to unpredictable power fluctuations.
- Smart Grid technology (specifically SCADA and SDX service) facilitates the collection of power measurements.
The transition to the Smart Grid introduces new regulatory considerations, which may transcend jurisdictional boundaries and require increased coordination among federal, state, and local lawmakers and regulators. The conceptual model is intended to be a useful tool for regulators at all levels to assess how best to achieve public policy goals that, along with business objectives, motivate investments in modernizing the nation’s electric power infrastructure and building a clean energy economy.

Therefore, the conceptual model must be consistent with the legal and regulatory framework and support its evolution over time. Similarly, the standards and protocols identified in the framework must align with existing and emerging regulatory objectives and responsibilities.

Figure 3-1. Interaction of Actors in Different Smart Grid Domains

through Secure Communication

Our focus
The transition to the Smart Grid introduces new regulatory considerations, which may transcend jurisdictional boundaries and require increased coordination among federal, state, and local lawmakers and regulators. The conceptual model is intended to be a useful tool for regulators at all levels to assess how best to achieve public policy goals that, along with business objectives, motivate investments in modernizing the nation's electric power infrastructure and building a clean energy economy. Therefore, the conceptual model must be consistent with the legal and regulatory framework and support its evolution over time. Similarly, the standards and protocols identified in the framework must align with existing and emerging regulatory objectives and responsibilities.

Figure 3-1. Interaction of Actors in Different Smart Grid Domains through Secure Communication

Our focus
3.3.2. Description of Conceptual Model

The conceptual model described here provides a high-level, overarching perspective of a few major relationships that are developing across the smart grid domains. It is not only a tool for identifying actors and possible communications paths in the Smart Grid, but also a useful way for identifying potential intra- and inter-domain interactions, as well as the potential applications and capabilities enabled by these interactions. The conceptual model represented in Figure 3-1 and Figure 3-2 is intended to aid in analysis by providing a view of the types of interaction development that are at the core of developing architectures for the Smart Grid; it is not a design diagram that defines a solution and its implementation. Architecture documentation goes much deeper than what is illustrated here, but stops short of specific design and implementation detail. In other words, the conceptual model is descriptive and not prescriptive. It is meant to foster understanding of Smart Grid operational intricacies but not meant to prescribe how a particular stakeholder will implement the Smart Grid.
3.3.2. Description of Conceptual Model

The conceptual model described here provides a high-level, overarching perspective of a few major relationships that are developing across the smart grid domains. It is not only a tool for identifying actors and possible communications paths in the Smart Grid, but also a useful way for identifying potential intra- and inter-domain interactions, as well as the potential applications and capabilities enabled by these interactions. The conceptual model represented in Figure 3-1 and Figure 3-2 is intended to aid in analysis by providing a view of the types of interaction development that are at the core of developing architectures for the Smart Grid; it is not a design diagram that defines a solution and its implementation. Architecture documentation goes much deeper than what is illustrated here, but stops short of specific design and implementation detail. In other words, the conceptual model is descriptive and not prescriptive. It is meant to foster understanding of Smart Grid operational intricacies but not meant to prescribe how a particular stakeholder will implement the Smart Grid.
3.3.2. Description of Conceptual Model

The conceptual model described here provides a high-level, overarching perspective of a few major relationships that are developing across the smart grid domains. It is not only a tool for identifying actors and possible communications paths in the Smart Grid, but also a useful way for identifying potential intra- and inter-domain interactions, as well as the potential applications and capabilities enabled by these interactions. The conceptual model represented in Figure 3-1 and Figure 3-2 is intended to aid in analysis by providing a view of the types of interaction development that are at the core of developing architectures for the Smart Grid; it is not a design diagram that defines a solution and its implementation. Architecture documentation goes much deeper than what is illustrated here, but stops short of specific design and implementation detail. In other words, the conceptual model is descriptive and not prescriptive. It is meant to foster understanding of Smart Grid operational intricacies but not meant to prescribe how a particular stakeholder will implement the Smart Grid.

Figure 3-2. Conceptual Reference Diagram for Smart Grid Information Networks
3.3.2. Description of Conceptual Model

The conceptual model described here provides a high-level, overarching perspective of a few major relationships that are developing across the smart grid domains. It is not only a tool for identifying actors and possible communications paths in the Smart Grid, but also a useful way for identifying potential intra- and inter-domain interactions, as well as the potential applications and capabilities enabled by these interactions. The conceptual model represented in Figure 3-1 and Figure 3-2 is intended to aid in analysis by providing a view of the types of interaction development that are at the core of developing architectures for the Smart Grid; it is not a design diagram that defines a solution and its implementation. Architecture documentation goes much deeper than what is illustrated here, but stops short of specific design and implementation detail. In other words, the conceptual model is descriptive and not prescriptive. It is meant to foster understanding of Smart Grid operational intricacies but not meant to prescribe how a particular stakeholder will implement the Smart Grid.
Replay Attacks

- “At a global scale, pretty much every single industrial or military facility that uses industrial control systems ... is dependent on its network of contractors, many of which are very good at narrowly defined engineering tasks, but lousy at cybersecurity.”

- “[conventional hackers] are also much more likely to go after civilian critical infrastructure. Not only are these systems more accessible, but they’re standardized ... all modern plants operate with standard industrial control system architectures and products from just a handful of vendors per industry .... ”

  R. Langner, cyberdefense consultant.

- As of 2010, more than 50,000 Windows computers infected.
Replay Attacks

Stuxnet Worm

**HOW STUXNET WORKED**

1. **infection**
   Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. **search**
   Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. **update**
   If the system isn’t a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. **compromise**
   The worm then compromises the target system’s logic controllers, exploiting “zero day” vulnerabilities—software weaknesses that haven’t been identified by security experts.

5. **control**
   In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. **deceive and destroy**
   Meanwhile, it provides false feedback to outside controllers, ensuring that they won’t know what’s going wrong until it’s too late to do anything about it.
Replay Attacks

Stuxnet Worm

**HOW STUXNET WORKED**

1. **infection**
   Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. **search**
   Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. **update**
   If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. **compromise**
   The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. **control**
   In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. **deceive and destroy**
   Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Replay attack at the cyber-physical interface
Replay Attacks

Small sample of existing work


- T. Tran, O. Shin, and J. Lee, “Detection of replay attacks in smart grid systems”, *IEEE 2013 International Conference ComManTel*

- F. Miao, M. Pajic, and G.J. Pappas, “Stochastic game approach for replay attack detection,” *2013 IEEE Annual Conference on Decision and Control*


- Y. Mo, R. Chabukswar, and B. Sinopoli, “Detecting Integrity Attacks on SCADA Systems”, *IEEE Transactions on Control Systems Technology*
Replay Attacks on SCADA Systems

(Mo, Chabukswar, and Sinopoli): LQG+$\chi^2$ Detector
Replay Attacks on SCADA Systems

(Mo, Chabukswar, and Sinopoli): LQG+$\chi^2$ Detector
Replay Attacks on SCADA Systems

(Mo, Chabukswar, and Sinopoli): LQG+$\chi^2$ Detector
Replay Attacks on SCADA Systems

(Mo, Chabukswar, and Sinopoli): LQG+$\chi^2$ Detector

$$u = u^* + \Delta u$$

Optimal LQG control

Authentication

$$y - \hat{y}$$

Innovation

Estimator

$\hat{y}$

Measurements

$y$

Controller

Delay

Attacker

monitor/control

Detector

$\Delta u' = ... + B\Delta u'_{k}$. (29)

Hence,

$$\hat{x}_k|_{k-1} - \hat{x}'_{k|_{k-1}} = A_k(\hat{x}_0|_{-1} - \hat{x}'_{0|_{-1}}) + \sum_{i=0}^{k-1} A_{k-i-1}B(\Delta u_{i} - \Delta u'_{i}).$$ (30)
Replay Attacks on SCADA Systems

Plant: \( x(t + 1) = Ax(t) + Bu(t) + w(t) \)
\( y(t) = Cx(t) + v(t) \)

Control Signal: \( u(t) = u^*(t) + \Delta u(t) \)
\( u^*(t) \): LQG optimal control signal.
\( \Delta u(t) \): Authentication signal with mean zero and covariance \( \mathcal{D} \).

LQG Performance: \( J = J_{LQG} + \text{trace} \{ (U + B'SB)\mathcal{D} \} \)

Detector: \( \sum_{t=k-T+1}^{k} (y(t) - \hat{y}(t))^\prime P^{-1} (y(t) - \hat{y}(t)) \leq \text{threshold} \)
Replay Attacks on SCADA Systems

Tradeoff between detection rate and control performance for a temperature control system.
Replay Attacks

A Novel Approach

\[ d(t) \rightarrow u(t) \rightarrow \text{Plant} \rightarrow y(t) \rightarrow \eta(t) \]

\[ \alpha_u(t) \rightarrow v(t) \rightarrow \text{Controller} \rightarrow w(t) \rightarrow \alpha_y(t) \]
Replay Attacks

A Novel Approach

Model of Power Flow in the Grid

\[ \text{Operations} \]

\[ d(t) \quad u(t) \quad y(t) \quad \eta(t) \]

\[ \alpha_u(t) \quad v(t) \quad w(t) \quad \alpha_y(t) \]
Replay Attacks

A Novel Approach

Model of Power Flow in the Grid

Data Network

Operations

\[ d(t) \rightarrow u(t) \rightarrow \text{Plant} \rightarrow y(t) \rightarrow \eta(t) \]

\[ \alpha_u(t) \rightarrow v(t) \rightarrow \text{Controller} \rightarrow w(t) \rightarrow \alpha_y(t) \]
Replay Attacks

A Novel Approach

Model of Power Flow in the Grid

\[ \eta(t) = \eta_0(t) + \eta_c(t) \]

Data Network

Operations

\[ d(t) \quad u(t) \quad y(t) \]

\[ \alpha_u(t) \quad v(t) \quad w(t) \quad \alpha_y(t) \]
Replay Attacks

Plant: 
\[ P(z) = \tilde{M}(z)^{-1}\tilde{N}(z) = N(z)M(z)^{-1} \]

Controller: 
\[ K(z) = U_n(z)V_n(z)^{-1} \]

Attack: 
\[ w(t) = y(t - \tau_\alpha) + \eta(t - \tau_\alpha) \]

Detector: 
\[ s = V_n(q)^{-1}w(t) \]
\[ |\Phi_s(\omega) - I| \leq \text{threshold OR Is the PSD of } s(t) \text{ white?} \]
Replay Attacks

Refining the Detector

Large deviation of $||\Phi_s(\omega) - I||$ in most of the frequency range does not hold in engineering practice.

Several methods available to obtain estimate of the PSD of $s(t)$. 
Replay Attacks

**Refining the Detector**

Large deviation of $\|\Phi_s(\omega) - I\|$ in most of the frequency range does not hold in engineering practice. (Unless variance of communication noise is very large, which is undesirable)
Replay Attacks

**Refining the Detector**

Large deviation of $\|\Phi_s(\omega) - I\|$ in most of the frequency range does not hold in engineering practice. *(Unless variance of communication noise is very large, which is undesirable)*

Therefore focus on a particular frequency $\omega = \omega_h$. 

15 / 23
Replay Attacks

Refining the Detector

Large deviation of $||\Phi_s(\omega) - I||$ in most of the frequency range does not hold in engineering practice. (Unless variance of communication noise is very large, which is undesirable)

Therefore focus on a particular frequency $\omega = \omega_h$. (Where the gain of the loop transfer function is high)
Replay Attacks

Refining the Detector

Large deviation of $\|\Phi_s(\omega) - I\|$ in most of the frequency range does not hold in engineering practice. (Unless variance of communication noise is very large, which is undesirable)

Therefore focus on a particular frequency $\omega = \omega_h$. (Where the gain of the loop transfer function is high)

Refined Detector:

$$\Phi_s(\omega_h) = \begin{cases} 
\sigma_d^2, & \text{if no replay attack,} \\
\sigma_d^2 + 2\sigma_c^2 |V(e^{i\omega_h})|^{-2}, & \text{if replay attack is present}
\end{cases}$$

Several methods available to obtain estimate of the PSD of $s(t)$. 
Replay Attacks

Detection rate performance for a temperature control system.
Comparison

**Novel Approach**
- Control signal is not limited to LQG control, any controller that can be represented by a coprime factorization may be used.
- No need to inject authenticating noise to control signal which could affect performance.

**LQG + $\chi^2$ Detector**
- Control signal is limited to LQG control.
- Control performance is sacrificed, although appropriate choice of $\mathcal{D}$ may reduce loss in performance.
Conclusion

- We use the communication noise that exists in networked control systems for detecting the replay attack.
- A spectral estimation method is developed to estimate the spectrum of the received signal at the controller site at a specific frequency point.
- Its value or its filtered value differ between the presence and absence of the replay attack.
References

- Figure in slide 3 from [http://solutions.3m.com/wps/portal/3M/en_EU/SmartGrid/EU-Smart-Grid/](http://solutions.3m.com/wps/portal/3M/en_EU/SmartGrid/EU-Smart-Grid/)
- Figure in slides 5-6 from NIST Special Publication 1108R2
- Figure in slide 7 from [http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet](http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet)
Outline

Smart Grid

Smart Grid Security

Conclusion

References

Questions
Thank you for your attention!