

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

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.



Outline

Smart Grid

Smart Grid Security

Replay Attacks

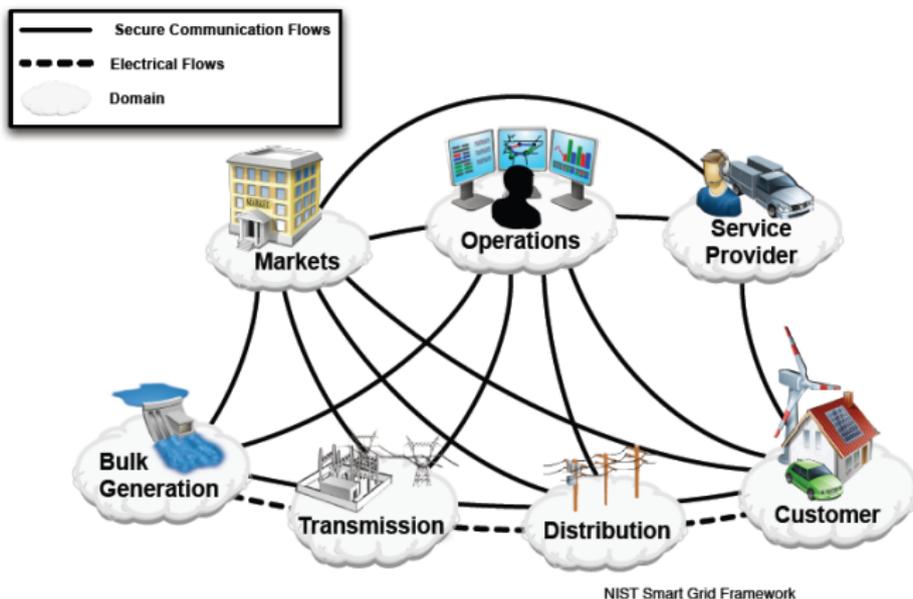
Conclusion

References

Questions

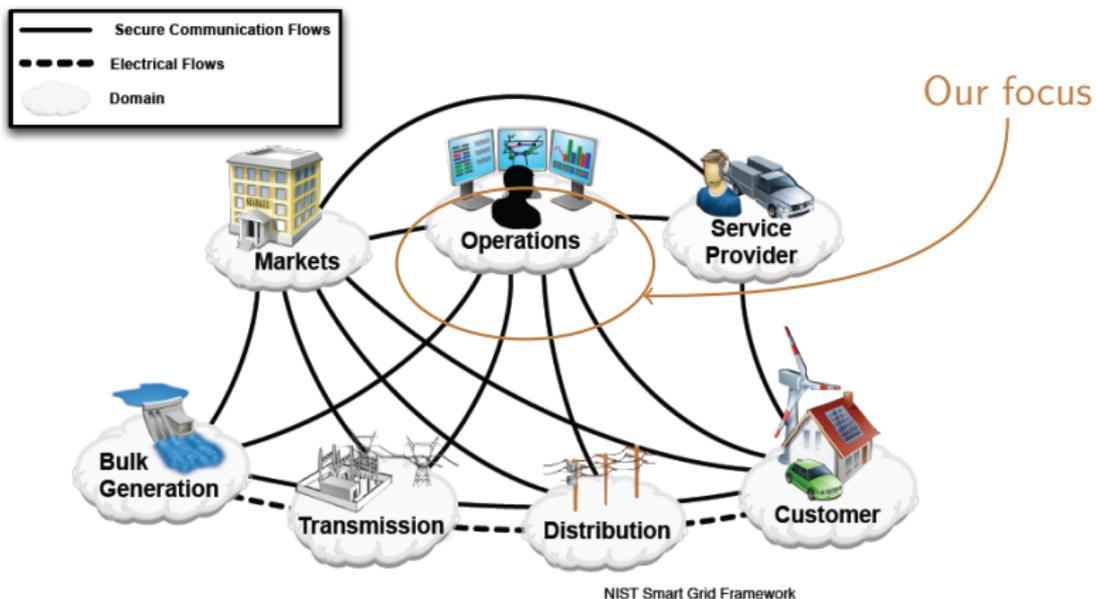
Smart Grid Security

NIST Conceptual Model



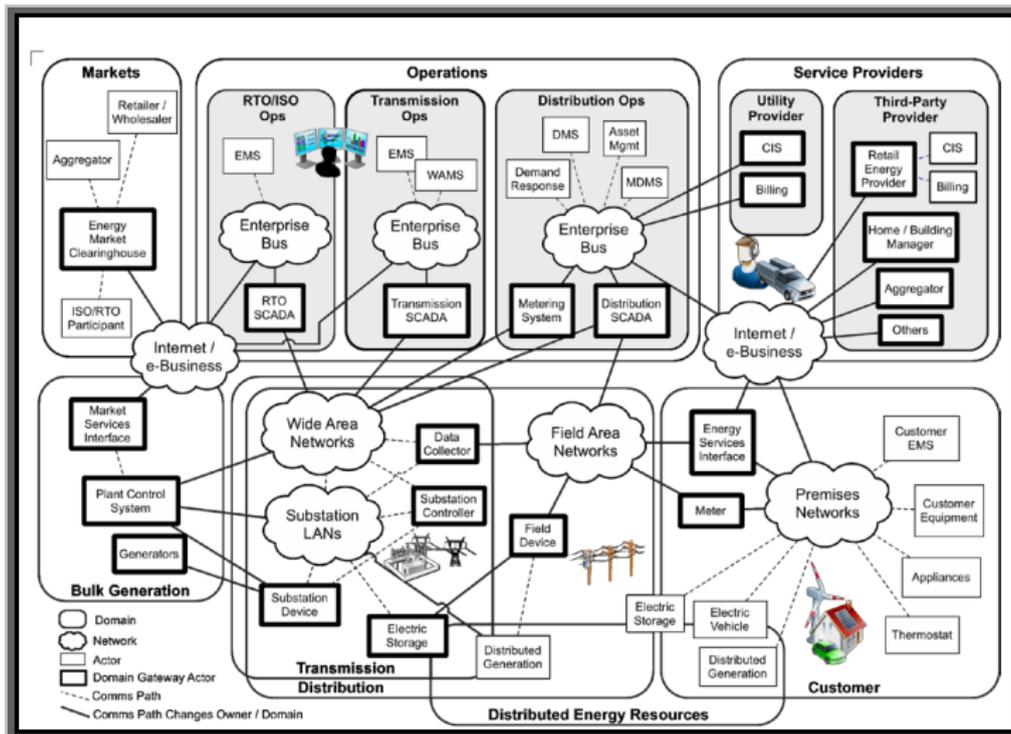
Smart Grid Security

NIST Conceptual Model



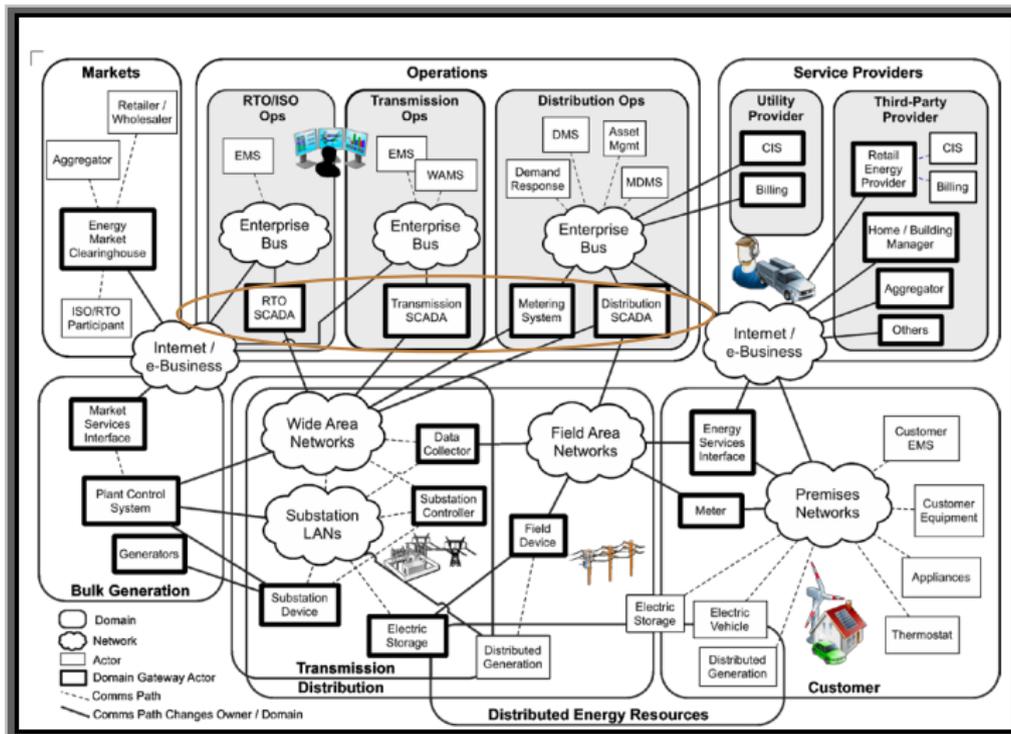
Smart Grid Security

NIST Conceptual Model Detail



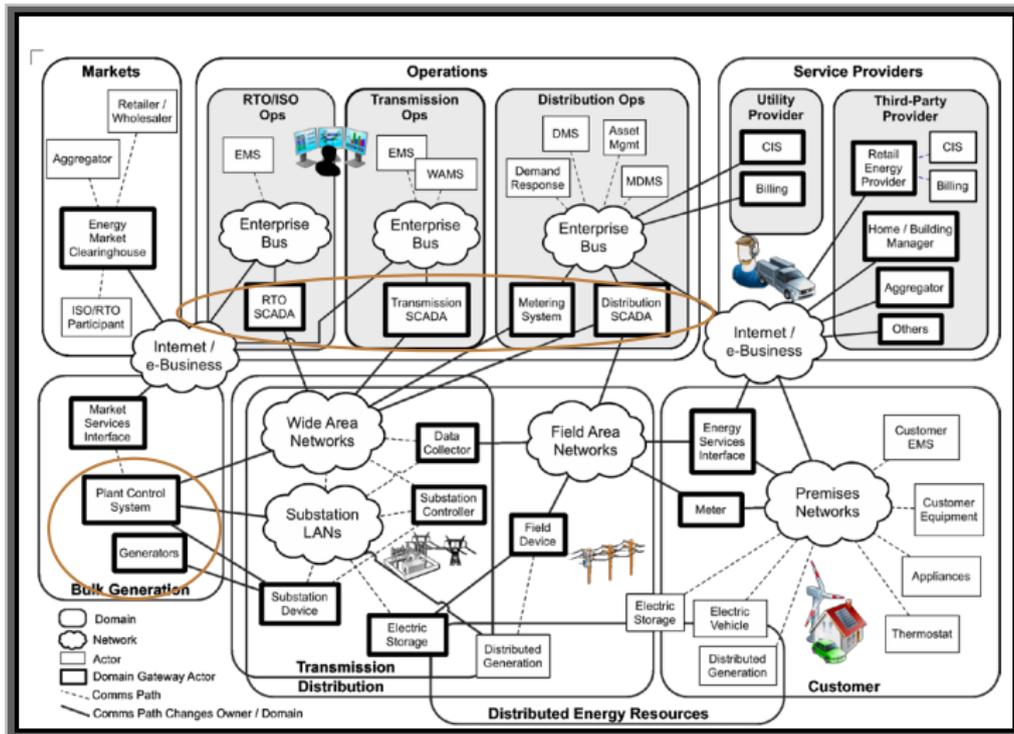
Smart Grid Security

NIST Conceptual Model Detail



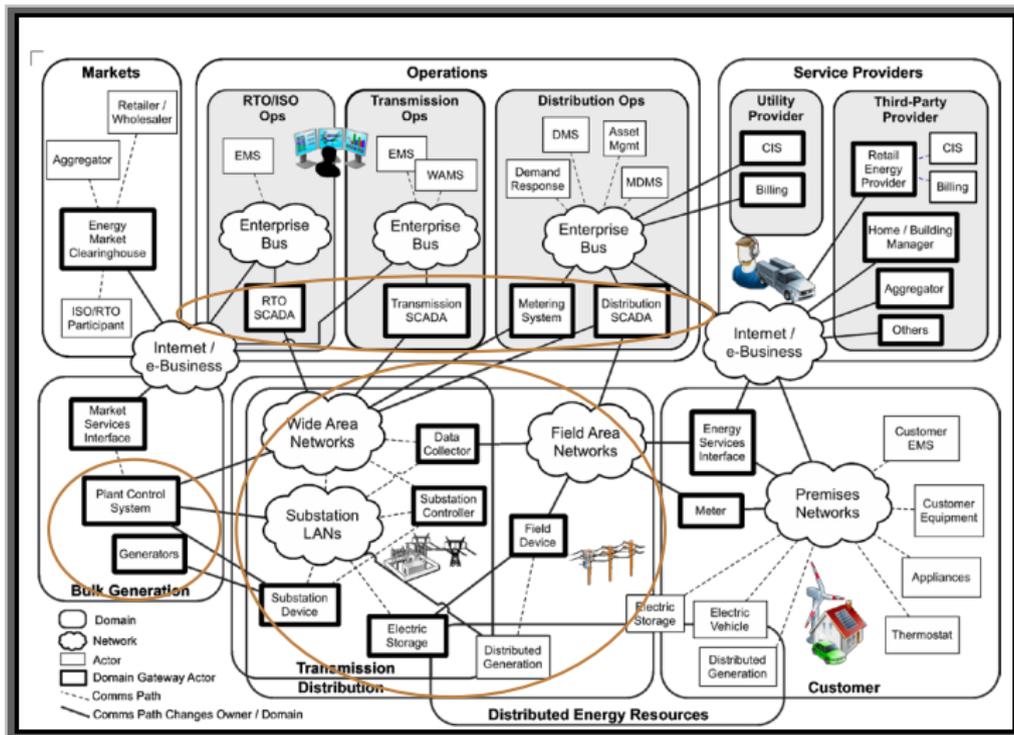
Smart Grid Security

NIST Conceptual Model Detail



Smart Grid Security

NIST Conceptual Model Detail



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.

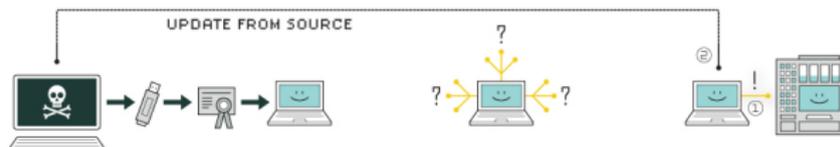
- ▶ As of 2010, more than **50,000** Windows computers infected.

The screenshot shows the New York Times website interface. At the top, the logo 'The New York Times' is on the left, and 'Middle East' is on the right. Below the logo is a navigation bar with categories: WORLD, U.S., N.Y. / REGION, BUSINESS, TECHNOLOGY, SCIENCE, HEALTH, SPORTS, and OPINION. Underneath that is a secondary navigation bar with regional categories: AFRICA, AMERICAS, ASIA PACIFIC, EUROPE, and MIDDLE EAST. The main article title is 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay'. The byline reads 'By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER' and the publication date is 'Published: January 15, 2011'. The article text begins with 'The Dimona complex in the Negev desert is famous as the heavily guarded heart of Israel's never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.' To the right of the text are social media sharing options: TWITTER, LINKEDIN, PRINT, REPRINTS, and SHARE. Below the text is a 'WATCH TRAILER' button. On the left side of the article, there is a photo of a man in a suit, identified as 'Ralph Langner, an independent computer security expert, solved Stuxnet.' Below the photo is a 'Multimedia' section.

Replay Attacks

Stuxnet Worm

HOW STUXNET WORKED



1. infection

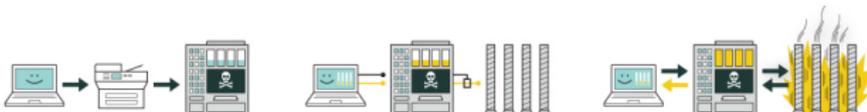
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

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.

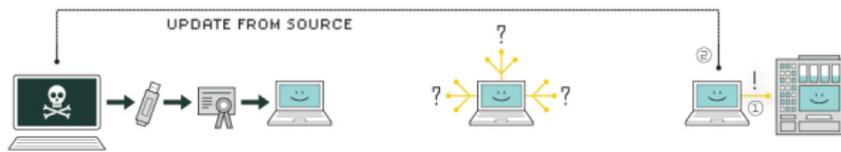
6. deceive and destroy

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.

Replay attack
at the
cyber-physical
interface



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.

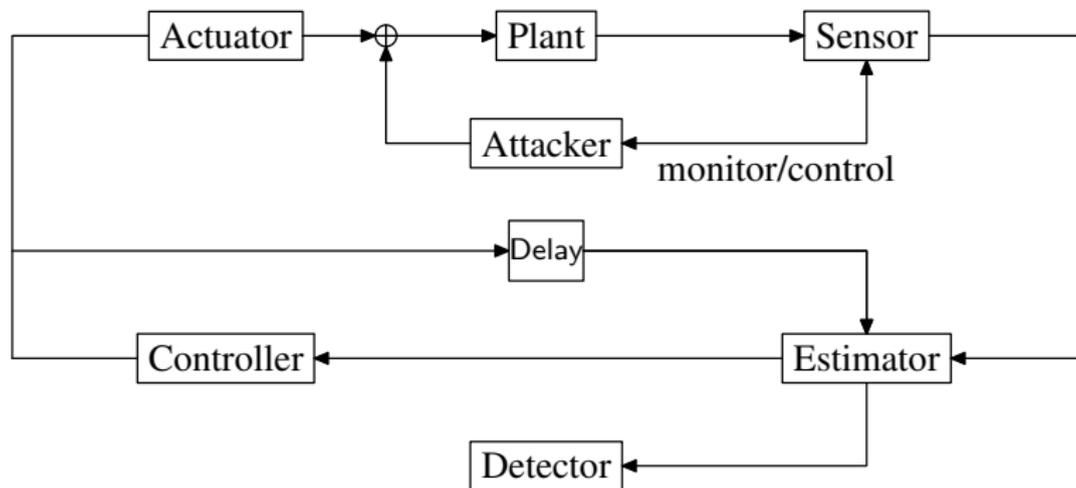
Replay Attacks

Small sample of existing work

- ▶ Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyberphysical security of a smart grid infrastructure," *Proceedings of the IEEE*
- ▶ 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*
- ▶ A.A. Cárdenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," *28th International Conference on Distributed Computing Systems Workshops*
- ▶ Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting Integrity Attacks on SCADA Systems", *IEEE Transactions on Control Systems Technology*

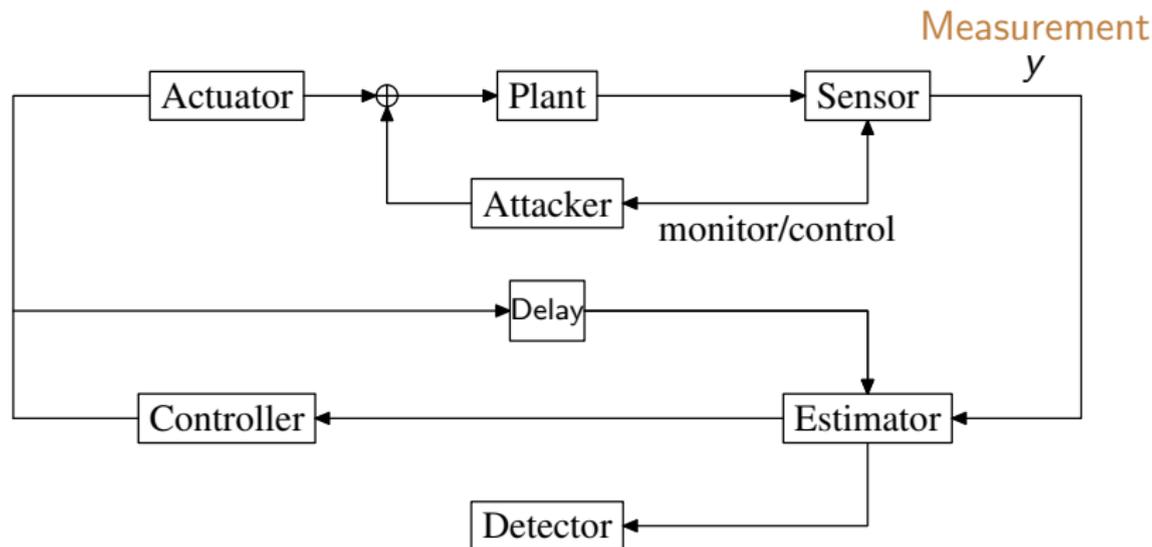
Replay Attacks on SCADA Systems

(Mo, Chabukswar, and Sinopoli): LQG+ χ^2 Detector



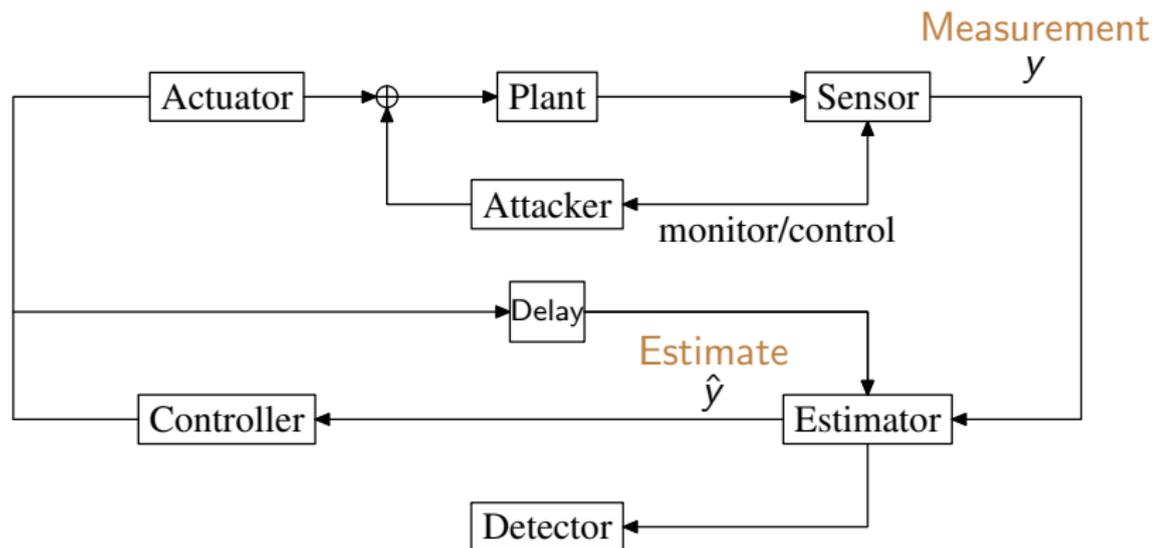
Replay Attacks on SCADA Systems

(Mo, Chabukswar, and Sinopoli): LQG+ χ^2 Detector



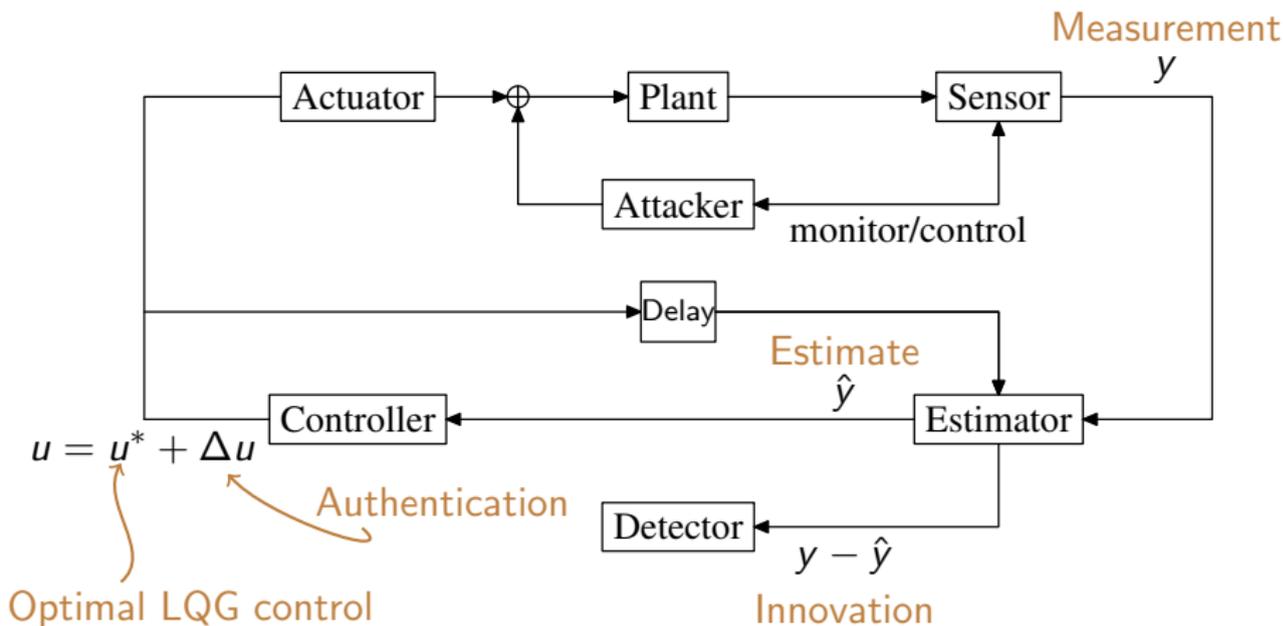
Replay Attacks on SCADA Systems

(Mo, Chabukswar, and Sinopoli): LQG+ χ^2 Detector



Replay Attacks on SCADA Systems

(Mo, Chabukswar, and Sinopoli): LQG+ χ^2 Detector



Replay Attacks on SCADA Systems

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

Control Signal: $u(t) = u^*(t) + \Delta u(t)$

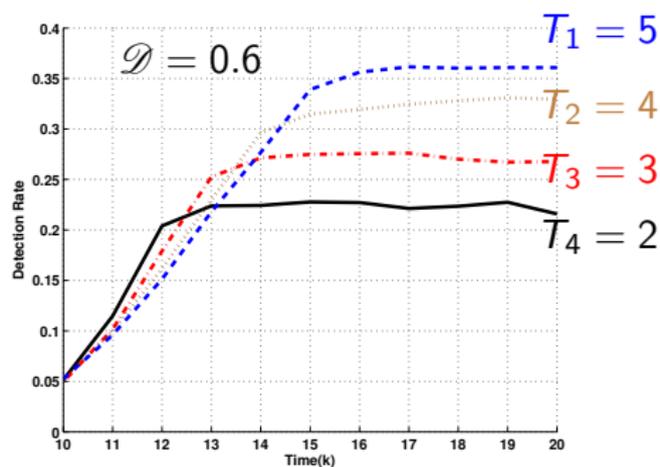
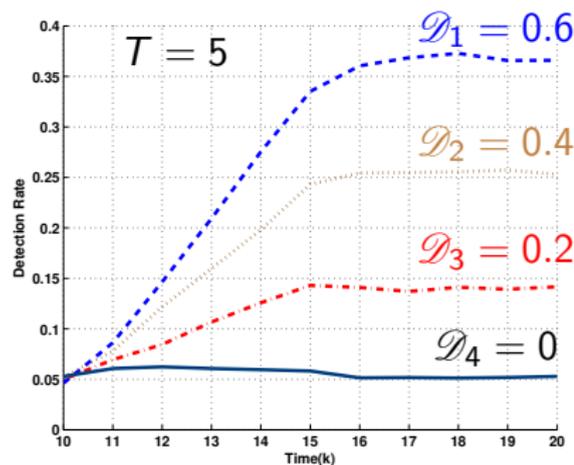
$u^*(t)$: LQG optimal control signal.

$\Delta u(t)$: Authentication signal with mean zero and covariance \mathcal{D} .

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

Detector: $\sum_{t=k-T+1}^k (y(t) - \hat{y}(t))' P^{-1} (y(t) - \hat{y}(t)) \leq \text{threshold}$

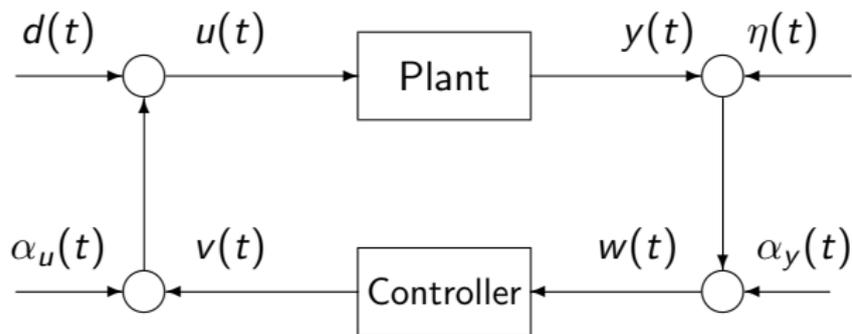
Replay Attacks on SCADA Systems



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

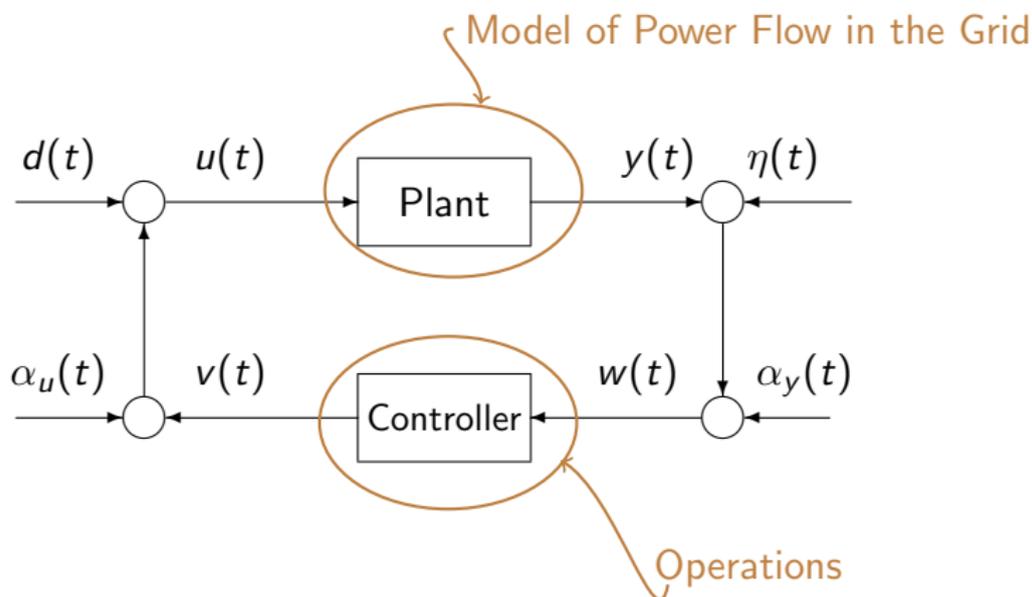
Replay Attacks

A Novel Approach



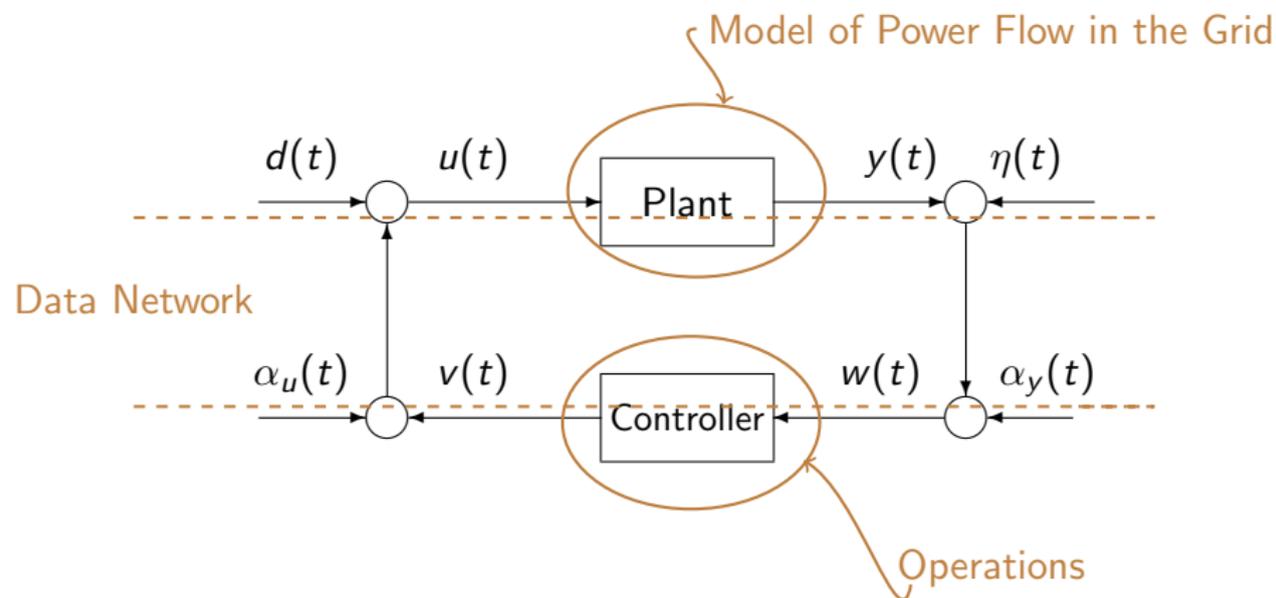
Replay Attacks

A Novel Approach



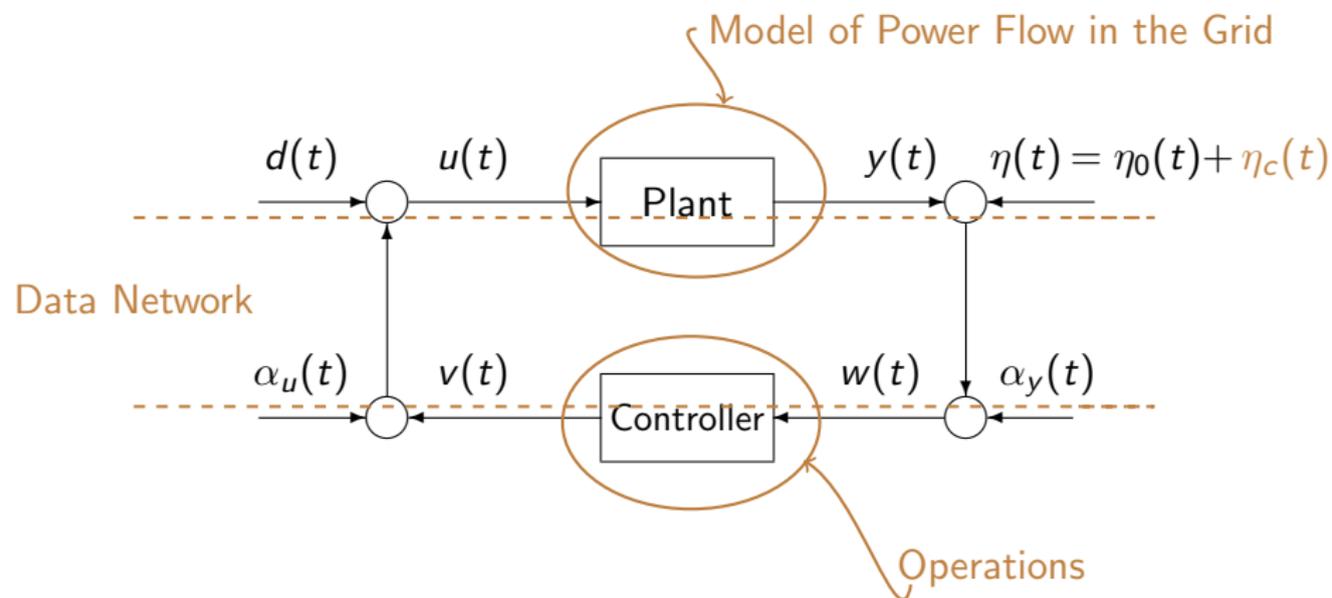
Replay Attacks

A Novel Approach

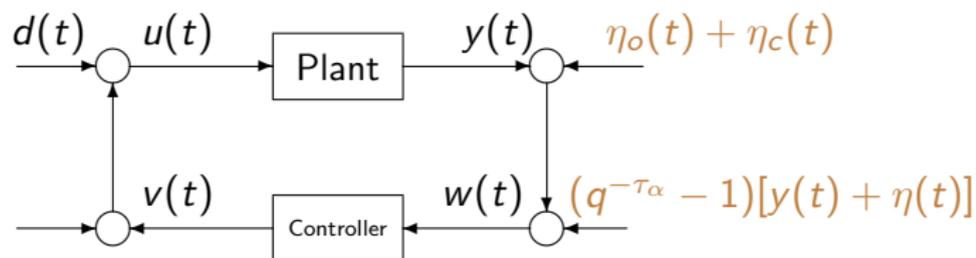


Replay Attacks

A Novel Approach



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 $s(t)$ 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.

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 $\omega = \omega_h$.

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)

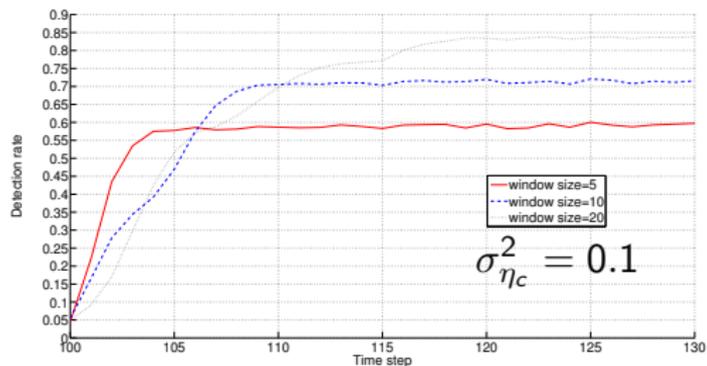
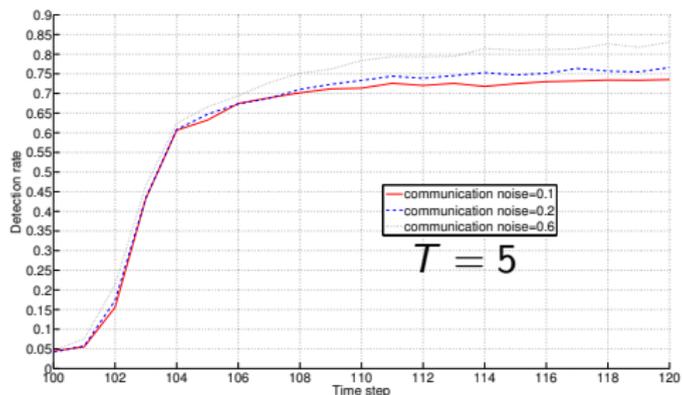
Therefore focus on a particular frequency $\omega = \omega_h$. (Where the gain of the loop transfer function is high)

Refined Detector:

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

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 + χ^2 Detector

- ▶ Control signal is limited to LQG control.
- ▶ Control performance is sacrificed, although appropriate choice of \mathcal{D} may reduce loss in performance.

Outline

Smart Grid

Smart Grid Security

Conclusion

References

Questions

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.

Outline

Smart Grid

Smart Grid Security

Conclusion

References

Questions

References

- ▶ Figure in slide 3 from 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>
- ▶ Y. Mo and B. Sinopoli, "Secure control against replay attacks," *Proceedings of 47th Annual Allerton Conference*, UIUC, IL, pp. 911-918, Sept 30 - Oct. 2, 2009.

Outline

Smart Grid

Smart Grid Security

Conclusion

References

Questions

Questions?

Thank you for your attention!