TCIPG

GridStat Middleware Communication Framework: Management Security and Trust

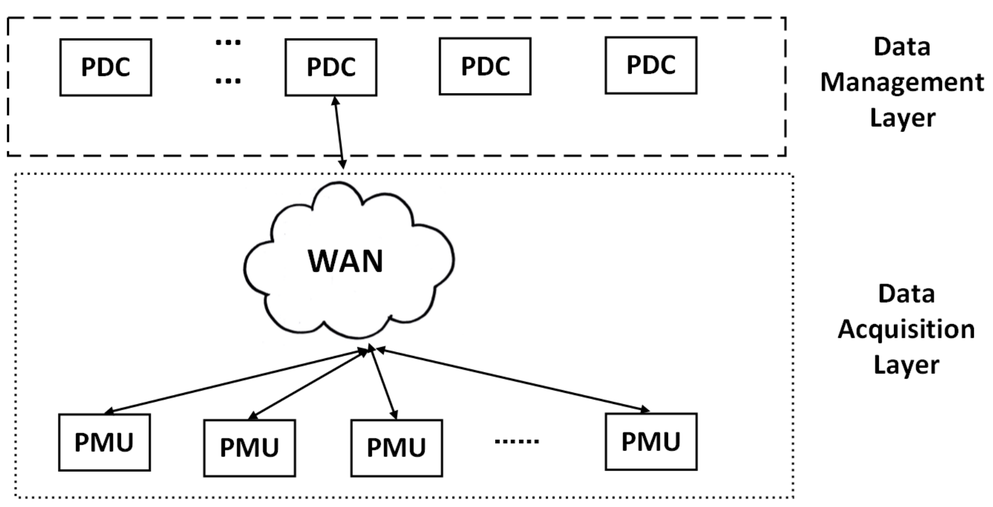
# Security Implications of Transport-Layer Protocols in Power Grid Synchrophasor Data Communication

Yujue Wang, Thoshitha Gamage, Carl Hauser

## GOALS

- Examine the communications between synchrophasors (PMUs) and phasor data concentrators (PDCs) to analyze potential security vulnerabilities present at the transport layer.
- Investigate the advantages and disadvantages of the TCP and UDP protocols, with an emphasis on security issues.
- Explore security implications of TCP and UDP underlying Transport Layer Security (TLS) and Datagram TLS (DTLS), respectively.
- Demonstrate attacks related to these security vulnerabilities in lab environment.
- Determine the requirements to launch these attacks and the complexities associated with committing them successfully.

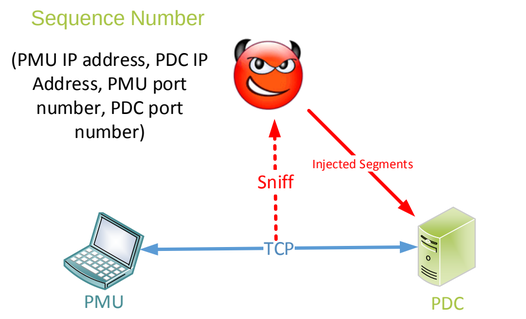
## FUNDAMENTAL QUESTIONS/CHALLENGES



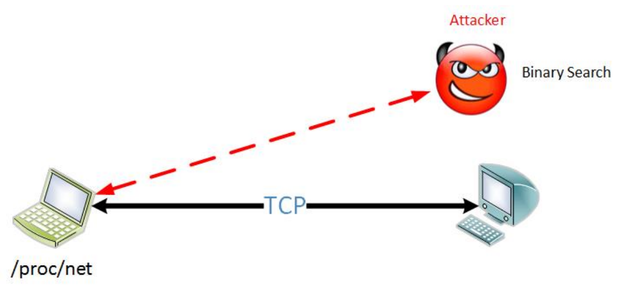

- Slight manipulation of timestamps, added delay or partial loss of data, or modest data tampering all could make the decision-making procedure dysfunctional and lead to incorrect or delayed decisions, affecting reliable and efficient operations of the power grid.
- Practical aspects of mounting cyber attacks on synchrophasor data communication are usually ignored.
- We inspected TLS and DTLS by exploring the security vulnerabilities of transport-layer protocols supporting them.

## RESEARCH PLAN

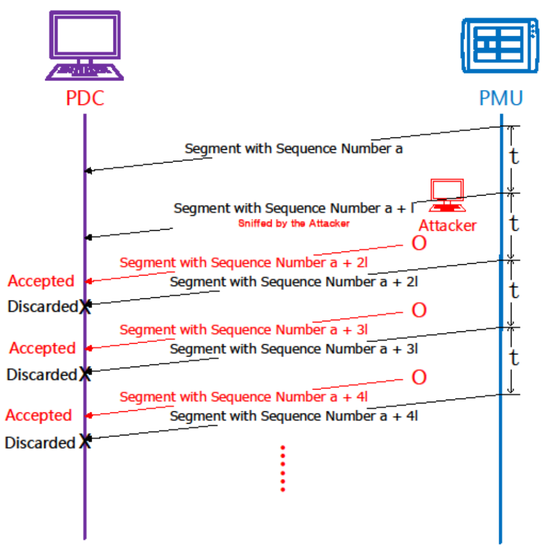
- Two kinds of attacks targeting plain UDP: inject IP-spoofed packets with false synchrophasor data; buffer flood.



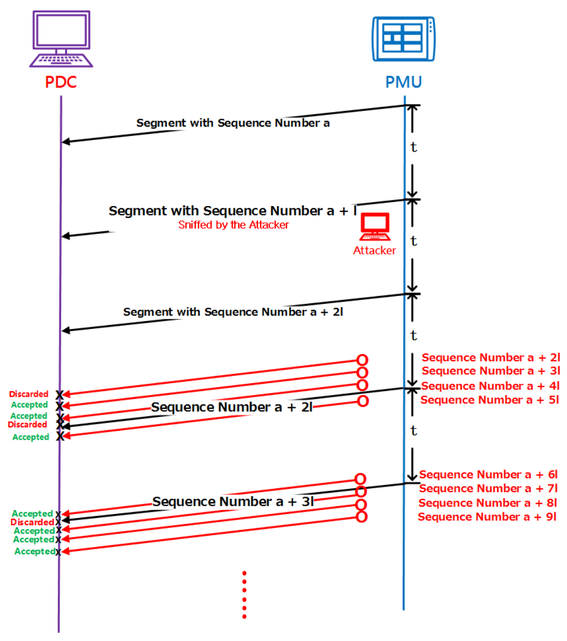

On-Path Injection




Off-Path Injection [1]




TCP Injection with a Pace-Tracking Attacker

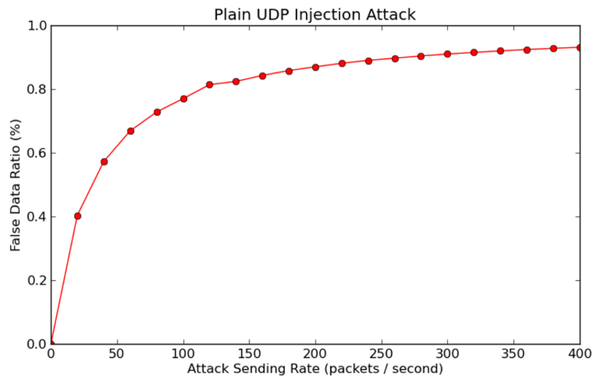



TCP Injection with an Extensive Attacker

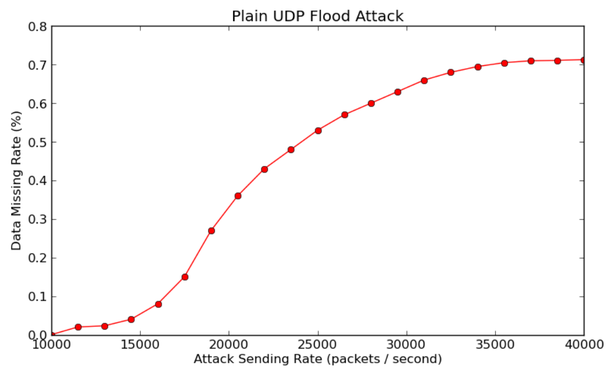
- Two kinds of attacks against TCP: pace-tracking and extensive.
- Same attacks as above on communications using TLS and DTLS
- Analyze the requirements for attackers to mount these attacks.

## RESEARCH RESULTS

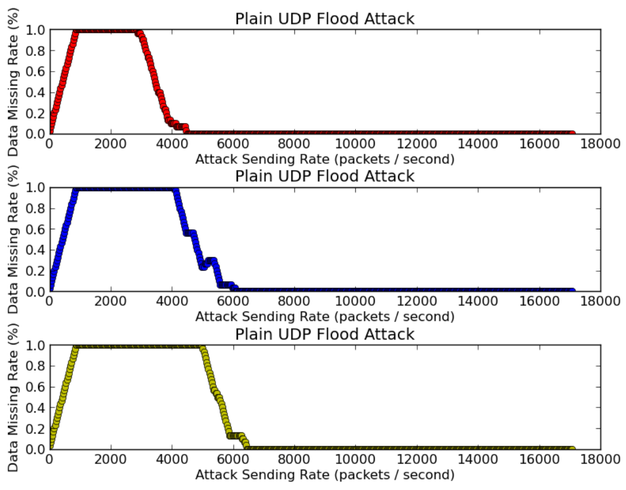
- PMU used in our experimental setup sends synchrophasor data at 30Hz following the format specified in C37.118-2011.
- We use Scapy to sniff packets and send arbitrary forged packets.



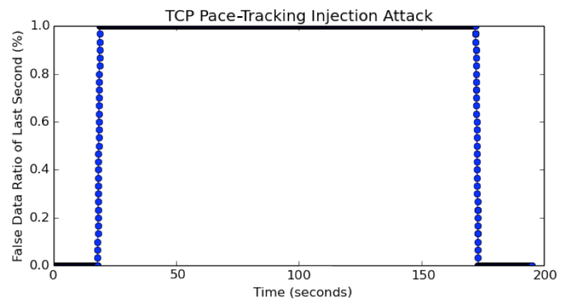

Plain UDP Buffer Flood Attack



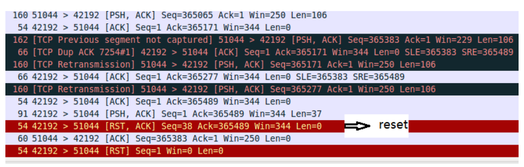

Plain UDP Injection Attack




TCP Injection with Extensive Attackers with Different Attack Windows




TCP Injection with a Pace-Tracking Attacker




Sequence Number Attack against TLS

- DTLS could mitigate both data injection and buffer overflow concerns at the transport layer. As with TLS, the certificate system and key management scheme introduce administrative complexity.
- Resource requirements of possible attacks against transport-layer protocols can be categorized as follows:

Attackers' Capabilities

| | |
|---|---|
| A1 | The attacker is able to commit IP spoofing. |
| A2 | The attacker can inject packet with the same four tuple of (*source IP address, source port number, destination IP address, destination port number*) with legitimate PMU data packets. |
| A3 | The attacker can sniff traffic on the connection between a PMU and a PDC. |
| A4 | For a TCP connection, the attacker can infer appropriate sequence numbers with the available side channel information. |
| A5 | The attacker can obtain time references as accurate as time references used by synchrophasors. |

Categories of Attacks and Requirements

| Attack | Type | Minimal Requirement |
|---|---|---|
| UDP Buffer Flood | DoS | {A0, A1} |
| UDP Injection | False Data Injection | {A0, A1} |
| TCP Pace-Tracking | False Data Injection | {A0, A2, A4} or {A1, A1, A3, A4} |
| TCP Extensive | False Data Injection | {A0, A2} or {A0, A1, A3} |
| TCP Injection with TLS | DoS | {A0, A2} or {A0, A1, A3} |

## BROADER IMPACT

- Show a practical way to commit intentionally coordinated false data injection attacks.
- Provide insight into security implications of standard transport layer protocols for periodic sensor data streams.
- Present a concrete example of problems related to choosing appropriate protocols for sensor data streams.

## INTERACTION WITH OTHER PROJECTS

- Collaborating with WSU Smart Grid Demonstration Research and Investigation Lab researchers investigating impacts of false data injection attacks on power grids.

## FUTURE EFFORTS

- Apply this analysis to different sensor protocols and smart grid applications.
- Develop a general framework for choosing appropriate security mechanisms given different security, performance, and implementation constraints, as well as uncertainties associated with implementation quality and human fallibility.

[1] "Collaborative TCP Sequence Number Inference Attack: How to Crack Sequence Number under a Second," Zhiyun Qian, Z. Morley Mao, Yinglian Xie, in *Proceedings of the ACM Conference on Computer and Communications Security (CCS) 2012*, Raleigh, NC.


FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T