De-Synchronisation Attack Modelling in Real-Time Protocols Using Queue Networks: Attacking the ISO/IEC 61850 Substation Automation Protocol

James Wright

Dr. Stephen Wolthusen

Information Security Group

Royal Holloway University of London

james.wright.2015@rhul.ac.uk

&

stephen.wolthusen@rhul.ac.uk

October 10, 2017

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Table of Contents

Defining our Problem

- Does the IEC 61850 and IEC 62351 standards meet the security and quality of service (QoS) promises laid out in its specification?
- If there are omissions, can they be exploited?
- Can these attacks still occur in a fully compliant implementation of the protocol?

The Protocol Problem

- The assumption in the research community is that the security and QoS promises of Smart Grid communications protocols are consistent throughout. However, there is little work on verifying them.
- No one has checked if the security promises come into conflict with the QoS requirements.
- Making sure that these promises are true could prevent some theorised attacks.

Table of Contents

Queuing Theory in Security

- Queuing theory is good tool for modelling Denial of Service (DoS) attacks.
- Most DoS models provide limited insight as most of them rely on M/M/1 queues or Jackson Networks.
- However, there have been some features from the literature that have been included in the framework that is being developed.

Queuing Theory in Security

- Queuing theory is good tool for modelling Denial of Service (DoS) attacks.
- Most DoS models provide limited insight as most of them rely on M/M/1 queues or Jackson Networks.
- However, there have been some features from the literature that have been included in the framework that is being developed.

1. Split state spaces
2. Limited capacity queues
3. Non-exponential probability distributions.

Table of Contents

Overview

- The framework uses a network of truncated $M/M/1/K$ queues, which provides probabilistic state exploration methodology. The probabilities of which is calculated using continuous time Markov Chains (CTMC).
- The assumptions made by the framework are:-

Overview

- The framework uses a network of truncated $M/M/1/K$ queues, which provides probabilistic state exploration methodology. The probabilities of which is calculated using continuous time Markov Chains (CTMC).
- The assumptions made by the framework are:-
  1. First-In-First-Out (FIFO) discipline for processing packets.
  2. Uses the Blocked-at-Service discipline.
  3. The effective probability distribution describing the rate at which packets are processed and unblocked are exponential distributions, but the sum of the distributions isn't.
  4. That the transition between states is memoryless.

The Probability of Queuing Theory

- The unique probabilities of the steady state of the network can be found using the global balance equation, assuming the system's state is:-

The Probability of Queuing Theory

- The unique probabilities of the steady state of the network can be found using the global balance equation, assuming the system's state is:-
  1. Independent of time.
  2. Independent of the initial state vector.
  3. The system is ergodic.

The Probability of Queuing Theory

- The unique probabilities of the steady state of the network can be found using the global balance equation, assuming the system's state is:-
  1. Independent of time.
  2. Independent of the initial state vector.
  3. The system is ergodic.
- $$\sum_{j \in \mathcal{I}} \pi_j q_{ji} = \pi_j \sum_{j \in \mathcal{I}} q_{ij} \tag{1}$$
- $$\mathbf{0} = \boldsymbol{\pi} \boldsymbol{Q} \tag{2}$$
- $$\sum \pi_i = 1. \tag{3}$$

The Topological Space

- The framework must calculate the parameters that govern how each queue in the network performs.
- The framework assumes for each queue that $a + b \leq c$ & $a + b + w \leq K$. As well as packets not returning to previous queues.
- The exogenous parameters must be set for each node. They are:

The Topological Space

- The framework must calculate the parameters that govern how each queue in the network performs.
- The framework assumes for each queue that $a + b \leq c$ & $a + b + w \leq K$. As well as packets not returning to previous queues.
- The exogenous parameters must be set for each node. They are:

Parameter	Description
K_i	Maximum capacity
μ_i	Service rate
γ_i	External arrival rate
$\phi(i, 1)$	Average number of distinct target queues
p_{ij}	Probability of packet transmission

The Topological Space continued

The endogenous variables can be calculated using the non-linear equations:

The Topological Space continued

The endogenous variables can be calculated using the non-linear equations:

Variable	Description
$P(N_i = K_i) = \frac{(1-\rho_i)\rho_i^{K_i}}{1-\rho_i^{K_i+1}}$	Probability of being full
$\lambda_i = \frac{\lambda_i^{eff}}{1-P(N_i=K_i)}$	Total arrival rate
$\lambda_i^{eff} = \gamma_i(1 - P(N_i = K_i)) + \sum_j p_{ji}\lambda_j^{eff}$	Effective arrival rate
$\mathcal{P}_i = \sum_j p_{ij} P(N_j = K_j)$	Probability being blocked
$\frac{1}{\widetilde{\mu_i^a}} = \sum_{j\in\mathcal{I}^+} \frac{\lambda_j^{eff}}{\lambda_i^{eff}\mu_j^{eff}}$	Common acceptance rate
$\frac{1}{\mu_i^{eff}} = \frac{1}{\mu_i} + \frac{\mathcal{P}_i}{\widetilde{\mu_i^a}\phi(i,1)}$	Effective service rate

The State Space

- The framework state space shows the probability of the each queue having a specific number of packets.

$$\mathcal{I} = \{(k_1, ..., k_N) \in \mathbb{N}^N\} \tag{4}$$

- In this state space there are three types of transitions between states:

The State Space

- The framework state space shows the probability of the each queue having a specific number of packets.

$$\mathcal{I} = \{(k_1, ..., k_N) \in \mathbb{N}^N\} \tag{4}$$

- In this state space there are three types of transitions between states:

Initial state s	New state t	Rate q_{st}	Conditions
$(i, ...)$	$(i+1, ...)$	λ_i	$p_{0i} \neq 0$ & $N_i \leq k_i - 1$
$(..., i)$	$(..., i-1)$	μ_i^{eff}	$p_{0i} \neq 0$ & $N_i \geq 1$
$(..., i, ..., j, ...)$	$(..., i-1, ..., j+1, ...)$	μ_i^{eff}	$p_{ij} \neq 0$ & $N_i \geq 1$ & $N_j \leq k_i - 1$

The State Space

- The framework state space shows the probability of the each queue having a specific number of packets.

$$\mathcal{I} = \{(k_1, \dots, k_N) \in \mathbb{N}^N\} \tag{4}$$

- In this state space there are three types of transitions between states:

Initial state s	New state t	Rate q_{st}	Conditions
$(i, \dots)$	$(i+1, \dots)$	λ_i	$p_{0i} \neq 0$ & $N_i \leq k_i - 1$
$(\dots, i)$	$(\dots, i-1)$	μ_i^{eff}	$p_{0i} \neq 0$ & $N_i \geq 1$
$(\dots, i, \dots, j, \dots)$	$(\dots, i-1, \dots, j+1, \dots)$	μ_i^{eff}	$p_{ij} \neq 0$ & $N_i \geq 1$ & $N_j \leq k_i - 1$

- The marginal probability in this state space is

$$\pi_i(k) = \sum \pi(k_1, \dots, k_N) \tag{5}$$

Performance Metrics

- From the marginal probabilities performance metrics can be calculated.

Performance Metrics

- From the marginal probabilities performance metrics can be calculated.

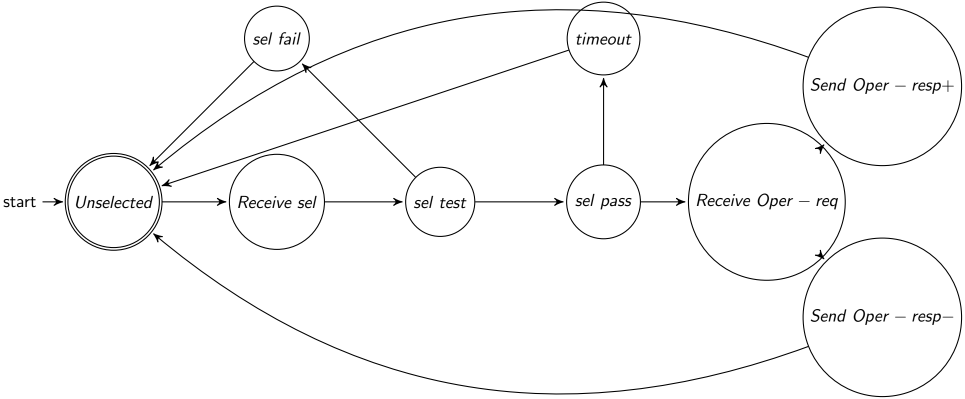
Performance Metric	Equation
Traffic Intensity	$\rho_i = \sum_{k=1}^{k} \pi_i(k)$
Throughput	$\lambda_i = \sum_{k=1}^{k} \pi_i(k)\mu_i^{eff}$
Total Throughput	$\lambda = \sum_{i=1}^{N} \lambda_{0i}$
Mean Number of Packets	$\bar{k}_i = \sum_{k=1}^{k} k\pi_i(k)$
Mean Queue Length	$\bar{q}_i = \sum_{k=c_i}^{k} (k - c_i)\pi_i(k)$
Mean Response Time	$\bar{T}_i = \frac{\bar{k}_i}{\lambda_i}$
Mean Wait Time	$\bar{W}_i = \bar{T}_i - \frac{1}{\mu_i^{eff}}$
Mean Number of visits	$e_i = \frac{\lambda_i}{\lambda}$
Relative Utilisation	$x_i = \frac{e_i}{\mu_i^{eff}}$

Table of Contents

The Setup - Part 1

- The attack causes the client's and server's state machines to become de-synchronised.
- This is achieved by either increasing or decreasing the rate at which the server receives the $oper - req[TestOK]$ message.
- The de-synchronisation of state occurs because the standard can be interpreted as not requiring the server to send out a *timeout* message to the client.
- The adversary in this attack is the same the symbolic one described by Dolev-Yao model.

The Setup - Part 2



The Result

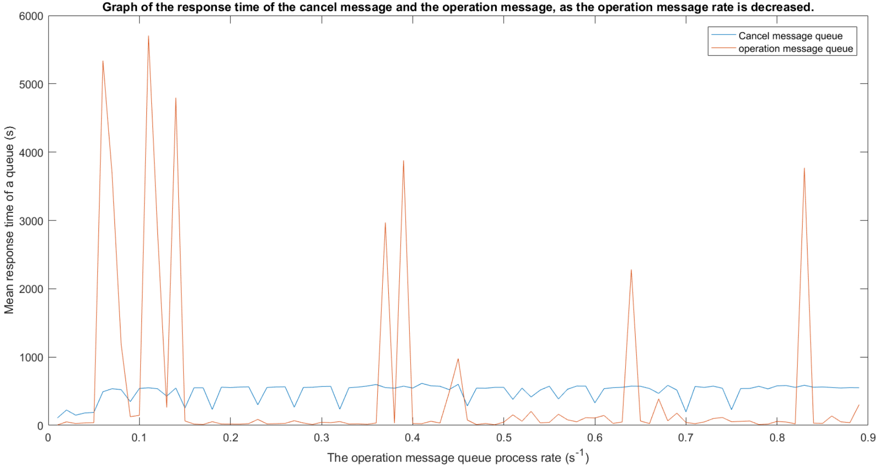

Graph of the response time of the cancel message and the operation message, as the operation message rate is decreased.
Cancel message queue
operation message queue
Mean response time of a queue (s)
The operation message queue process rate (s^{-1})
0
1000
2000
3000
4000
5000
6000
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9

Table of Contents

Future Direction-Framework

- Include the ability to calculate conditional probabilities of events.
- Include state spaces of the possible internal states of each queue.
- Include packet dropping in the model.

Future Direction-Analysis

- Develop weaker adversary models.
- Generate a taxonomy of attacks against Smart Grid protocols.
- Find instances of the attacks with IEC 61850 and IEC 62351.

Questions?