Developing a Framework to Address Performance and Security Protocol Concerns in Identity Management for Positive Train Control Systems

Andre Bondi, Siemens Corp., Corporate Research and Technology, Princeton, NJ

SIEMENS

Duminda Wijesekera,Damindra Bandara;
George Mason University, Fairfax, VA
Rajni Goel, Nalin Pilapitiya; Howard University, Washington DC

This work is supported by a grant from the Federal Railroad Administration, USDOT. Support does not consitute endorsement. The opinions are those of the authors.

Overview of Positive Train Control

- On-Board Units (OBU) in locomotives receive wireless messages regarding signal status, local speed restrictions, switch settings

- GPS used to show driver, back offices position of trains, signals
  - Rail area to be traversed by train stored in an on-board DB which is loaded onto the OBU before the train leaves its origin

- Trains move from one network to another, e.g. Amtrak/NJ Transit, Amtrak/SEPTA, BNSF/UP, CP/UP, etc.

- Each railroad controls its own network
  - Must communicate with all trains on its network
  - Need standardized interfaces, protocols, authentication.
- *Interoperability is essential to implement this.*

Security Criteria

1. C = confidentiality – No specified use case
2. I = Integrity = Message Integrity
3. A = Availability of the Information= Need to know by intended recipient
   - Security mechanisms cause performance costs - later
- (2) and (3) require authentication
- Revelations about terrorists' intent to attack trains underscore issue

- Solutions intended to counter threat models and scenarios

Security Details

- **Authentication**
  - Locomotives and host networks must mutually authenticate each other.
  - Signals, switches monitored locally by Wayside Interface Units (WIU)
  - *Does the train know that messages allegedly from WIUs really are?*
  - *Do WIUs know that messages allegedly from locomotives really are?*

- **Integrity**
  - Messages must have integrity:
    - what was sent ➔ what is received➔ messages not altered in transit

Performance Issues

- Can authentication/identity management occur fast enough to ensure timely delivery of signaling instructions to the locomotive?
- What are the performance requirements for Positive Train Control (PTC) identity management?

The answers to these questions are influenced by:

- The braking properties of trains, and how fast they travel
- The volume of train traffic (trains per hour through an area)
- The computer systems implementing PTC
- Properties of radio spectrum (220 MHz)
- Standards and regulations (draft or existing)
  - Federal Register and US codes;
    - Legislation (Congress) and Rulemaking (FRA)
  - American Association of Railroads standards
  - AREMA standards
  - Manufacturing standards

Research Objectives

- Provide a framework for predicting authentication delays given traffic and the characteristics of the devices and computer systems involved
- Develop set of performance requirements for identity management and authentication in Positive Train Control
- Identify the conditions under which the performance and safety requirements can be met, and their impact on train movements
- Study will lead to the development of parameters that could be used in network capacity planning and train scheduling

Current Status of System Under Study

Problem is open-ended:

- Characteristics of the computer systems involved are unknown
- Characteristics of radio transmission are unknown
- Authentication protocols not fully specified
  - Authentication messages not specified in Interoperable Train Control (ITC) Office-Locomotive Interface Control Document S9352-A

BUT: several use cases are known

Research Methodology and Framework

- Identify use and misuse cases for study and develop UML message sequence charts and activity diagrams for them, deployment diagrams
- Identify or devise authentication protocol meeting safety, security, and performance needs
  - *Must verify that all needs can be met simultaneously*
- Associate activities with deployment scenarios
- Devise straw architecture for performance study to provide a base line
- Build parameterized models that include hypothetical device, bandwidth characteristics
- Identify delay requirements based on postulated braking characteristics of trains
- Identify load characteristics and reference scenarios from information about a reference hub suburban station: train timetables, maps of track and signal layouts

Why Study Reference Station?

- Three passenger railroads converge on the reference station
  - Long distance
  - Two commuter lines
- Freight trains go through the reference station
- All use the same tracks
- It is large enough to be interesting but not so large as to be difficult to study

Performance Requirement: Response Time
Braking Properties: Stopping Distance

- Braking curves show speed vs. *distance*
- How do we get from distance to *response time*?
- Some mathematics required.
- Need to understand braking time so that we can specify response time requirement for
  - Authentication
  - Processing stop signal or green signal
- Default:
  - Train stops if it does not know what to do
  - *Undesirable if not necessary, because of energy cost and acceleration time.*

Braking curves

- Used to specify braking properties
- Speed as a function of distance traveled from first application of brakes

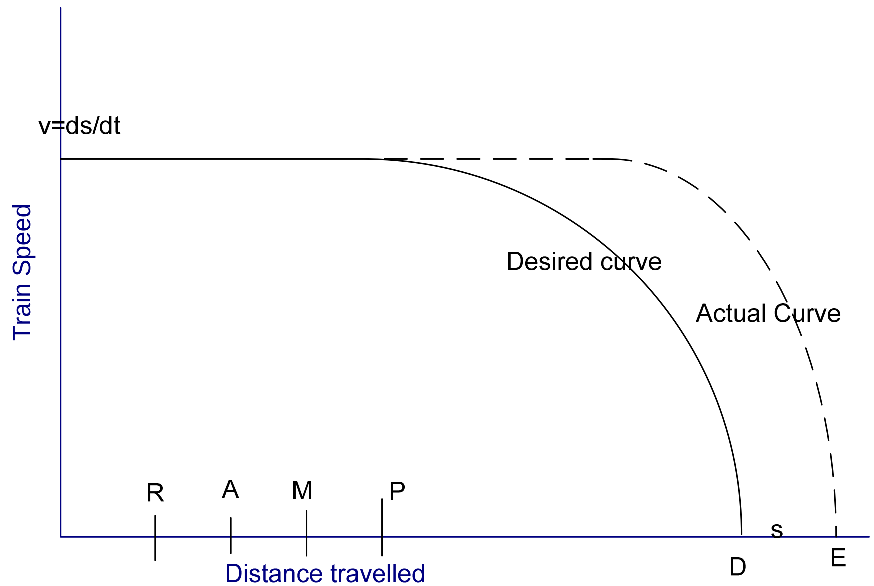
$$ds/dt = f(s)$$

$f(0) = v0$ initially

$f(D) = 0$ => train stopped entirely

$f(D) = v1 < v0$ => train slowed

- Solve to obtain times by separation of variables and integration to obtain times to travel between points 0, R, …, D on graph



More on Braking Curves

Dependent on

- Train characteristics
  - Nature of load
  - Type of train
  - Type of locomotive
- Terrain, environmental factors
  - Uphill, downhill
  - Open area
  - Approaching a station or yard
  - Approaching signal, points
  - Approaching work area
  - Weather (wet tracks, leaves, ice)
- Emergency vs. programmed stop
  - Don’t want to flatten the wheels!

Curve Formulation

- Stopping distances ~1 mile
- Continuous function, else abrupt movements!
- Open literature based on Newtonian mechanics
- Braking curves seldom published
  - Proprietary to train manufacturer
- May depend on driver reaction time, time to apply brakes along entire train
- Might be specified numerically rather than in closed form

Problem:
Braking curve speed=f(distance); performance requirement=g(time)

A Little Mathematics

- Speed related to distance and time
- Separation of variables problematic because f(s)=0 when the train has stopped.
- Solve numerically (mid-point approximation) to obtain approximate braking time
- *Braking time tells us how quickly signal information must be relayed to the train as function of speed and braking over distance*
- *Numerical method is general*

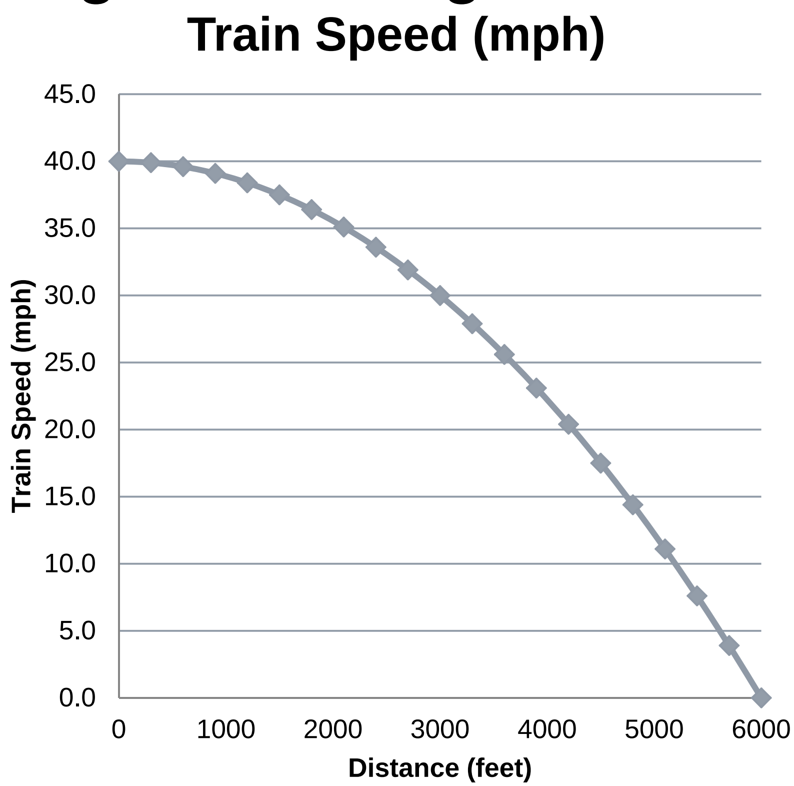
$$\frac{ds}{dt} = f(s)$$

$$\int_{s=R}^{s=E} \frac{ds}{f(s)} = \int_{t_R}^{t_E} dt = t_E - t_R$$

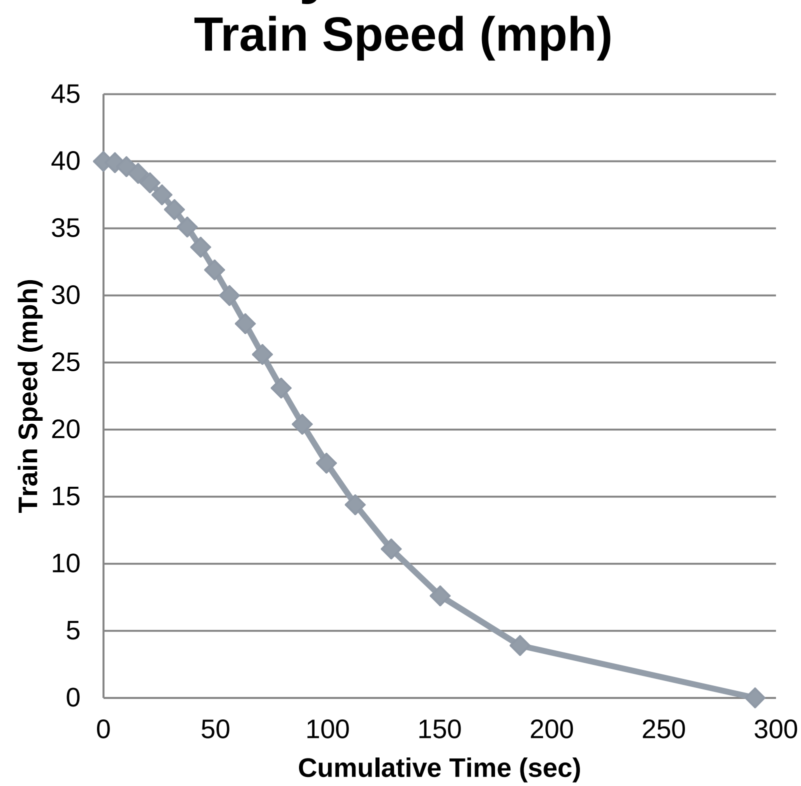
$$t_{i+1} \approx t_i + \gamma \frac{s_{i+1} - s_i}{[f(s_{i+1}) + f(s_i)]/2}, \quad i = 0, 1, \ldots, K-1$$

Example: Quadratic braking curve (arbitrary)

Original Braking Curve



Timings obtained numerically



From Braking Curve and Timetable to Performance Requirements

- Default action is to stop the train (fail safe mode),
  - Authentication must be fast enough to allow train to proceed if safe to do so
  - Avoids wear on brakes, track
  - Saves energy cost of getting train moving if stopped unnecessarily
- Authentication must be fast enough to bring train to a stop or slow it down when needed (emergency situation, work area)
- Look at implications for
  - Protocol processing
  - Back end databases
  - Business logic
- Additional requirement:
  - Track database downloaded into locomotive OBU before each journey within a specified time.

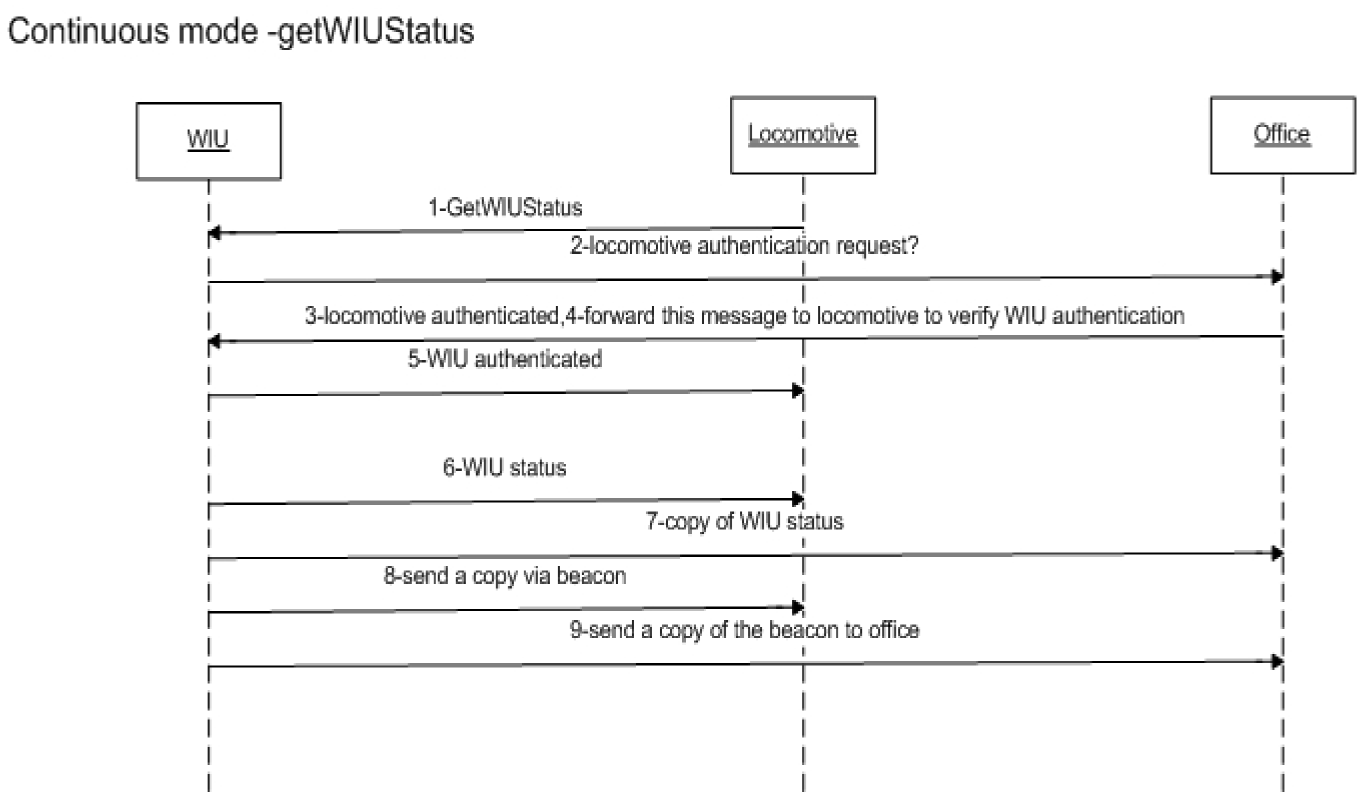
Examples of Use Cases

- Trains moving from one PTC-controlled network to another
- Trains moving from a PTC-controlled network to one that is not
- Trains moving from a non-PTC-controlled network to a PTC-controlled network
  - Non-PTC track segment may not have any signals at all: *dark territory*

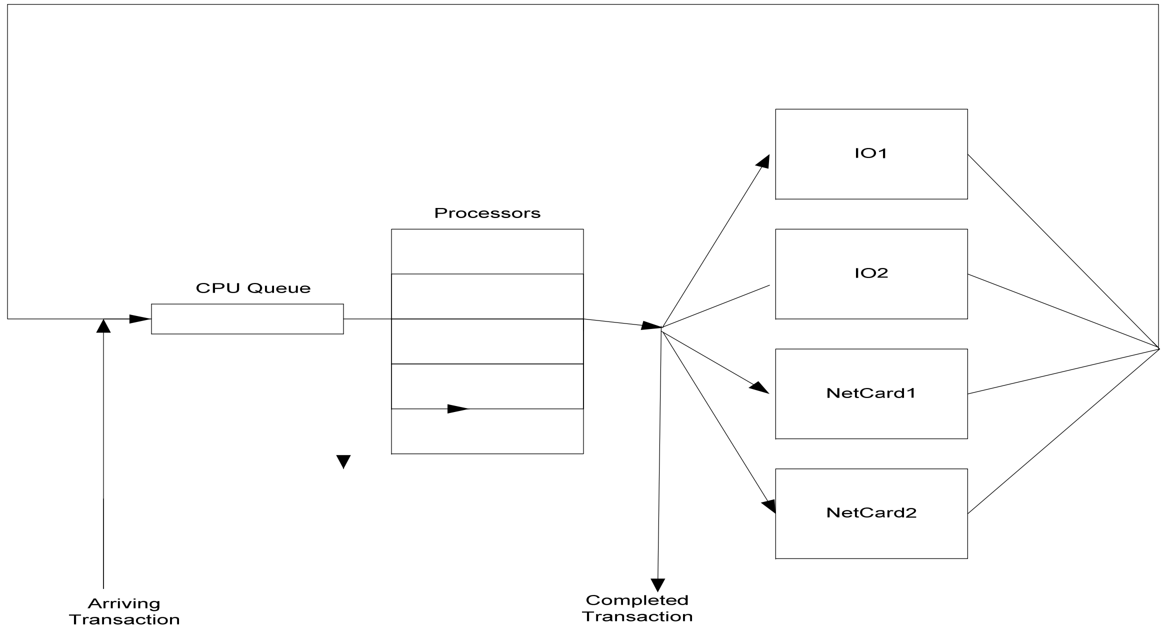
Variations:

- Train and network belong to the same carrier
  - Authentication simplified
- Train and network belong to different carriers (tenant train, host network)
  - Host network's back office must authenticate incoming train with tenant train owner's back office (compare with cell phone roaming)

Use Case: Locomotive approaching signal guarding PTC area from non-PTC area



Example Back Office Server



Modeling Approach I

- Map from use cases to resource usage model (based on measurements or estimates), stated hardware platforms
- Combine resource usage model with estimates of
  - Train movement frequency (based on time tables)
  - Knowledge of how many switch positions, signal indications must be altered given
    - train movements,
    - wayside devices connected to Wayside Interface Unit
- Obtain lower bounds on processing delays
- Obtain estimates of bandwidth demands, networking delays
- Compare with suggested requirements

Example Model Parameters for the Back Office Server (one column for each arrow in the message sequence chart)

Activity or Transaction Type	2- Locomotive Authentication Request	3- Locomotive Authentication Request (response)	7- Send copy of WIU status	9- Send a copy of the beacon to the BOS (repeated)
Incoming or outgoing?	Incoming	Outgoing	Incoming	Incoming
CPU time (msec)				
IO1 time (msec)				
Packets in/ transaction				
Packets out/ transaction				
Packet size (bytes)				
Transmission Time Card1 (msec)				
Total Transaction rate (per sec)				
UseCase1				
RateUseCase 1 (per sec)				
UseCase 2				
RateUSeCase2 (per sec)				
Radio propagation delay				

Modeling Approach II

- Build coarse, easily solved queueing model based on measurements and/or parameters (use expert intent when necessary)
- Vary parameters to determine sensitivity of results to parameter values
- Compare delays with performance requirements conditioned on train speed, train volume, distances of signals from brake activation points to determine if performance requirements are attainable.

Next Steps

- Identify model parameters to use in predicting performance
  - Processing times
  - Network transmission and propagation times for messages
  - I/O times
  - ….
- Choose parameters based on
  - Measurement where possible
  - Educated guesses where not possible
  - Network transmission delays obtainable from knowledge of bandwidth
  - Knowledge of packet volumes from use cases
- Build performance model