RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

Railway Cyber Risk Research
Entry Evaluation Task

Rutgers Rail Research Group
Civil and Environmental Engineering Department
Oct. 26th 2018

Railroad Transportation Traffic Modeling

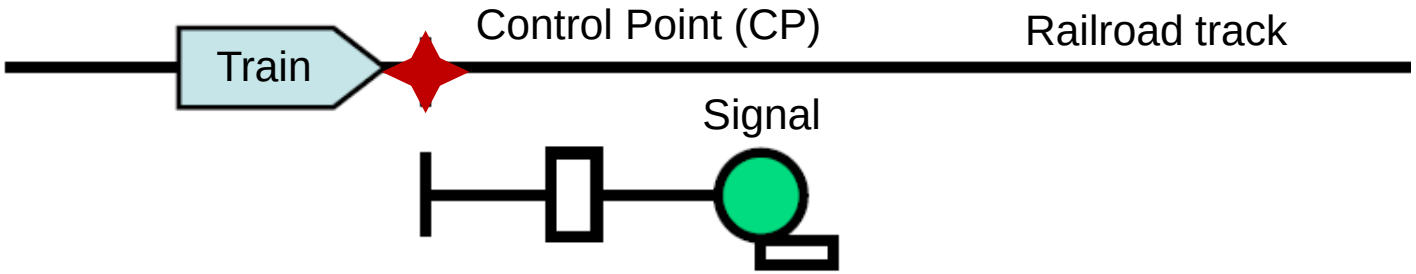
- Background Intro:
  - Railroads use wireless communication to remotely control signals for trains:
    - Train dispatchers monitor train activities remotely via certain wireless protocols;
    - Train dispatchers order “green, yellow, red” signals for trains at a certain location.
  - This task aims to evaluate the capability of researchers as to:
    - develop a **scalable model** to describe real train operations;
    - **Estimate the consequences** under simple types of cyber attack, as:
      - To jam the narrowband wireless channel to disable the remote signal;
      - To spoof the message to achieve malicious goals.

Railroad Transportation Traffic Modeling

- What you may do in the future & What you need to do now?
  - Selected researchers will join the team, and further evaluate various attack types and corresponding consequences, based on:
    - The concrete details of communication/network protocols that applied in the industry;
    - Their own expertise to support identifying the cyber vulnerabilities of railroad operations;
    - Build up the cyber risk evaluation tool for industrial customers to prioritize the urgent risk:
      - Translate cyber attacks into scalable probabilistic models;
      - Implement cost-effective countermeasures based on domain knowledge;
      - Prepare for the probabilistic risk model construction.
  - In this task, **try to jump a little out** of your current communication or network domain knowledge, but focus on the simulation and modeling:
    - Be practical to understand railroad operation following the descriptions;
    - Be creative and imaginative,
      - but don’t miss any explanation for your great ideas and assumptions!

Entry Task – Step 1

- Uni-directional Traffic Model:
  - Suppose a wireless **Control Point (CP)** at a railroad, whose signal(s) control a segment of railroad track. Dispatchers talk to CPs to order signal.



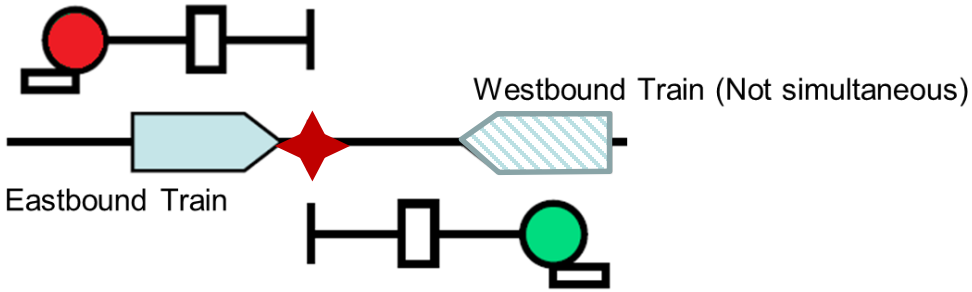
  - The traffic is **uni-directional**
  - A jamming DoS attack will trigger safemode of the CP, set all signals red only: This will stop all the trains from passing the CP, until the attack is resolved.
  - Simple assumption:
    - All trains will stop in time and not pass the attacked CP.
    - The next train won't come unless the previous train has passed the CP.
  - Objective:
    Quantify the train delay under a jamming DoS attack-and-solve cycle.

Entry Task – Step 1

- Base Parameters:
  - Annual train traffic: 500 Million-Gross-Tons (MGT):
    - Tip: MGT is the total weight for all trains in a year passing this signal point.
  - Weight of a train is following the standard distribution of:
    - N~(5000 tons, 1500 tons). Truncate the weight at minimum 1000 tons
  - Incorporate the train minimum spacing buffer time with a standard distribution of:
    - N~(15 minutes, 3 minutes). Truncate the buffer at minimum 8 minutes;
    - Tip: Adjacent trains have to be spaced in the buffer time for safety.
- Cyber Model Variables:
  - Cyber attack **duration** and **recover time**:
    - What if the jamming DoS **lasts for X hours**, and **recovery needs Y hours**;
    - Tip: Provide simple but reasonable estimation describing the attack.
- Expected Output: *(be scalable for future steps!)*
  - Traffic prediction/estimation in MGT under such DoS attack:
    - Sure less than 500 MGT, but how much if we play around the parameters and variables? (*say X=3, Y=5, or change the distribution, etc.)*

Entry Task – Step 2

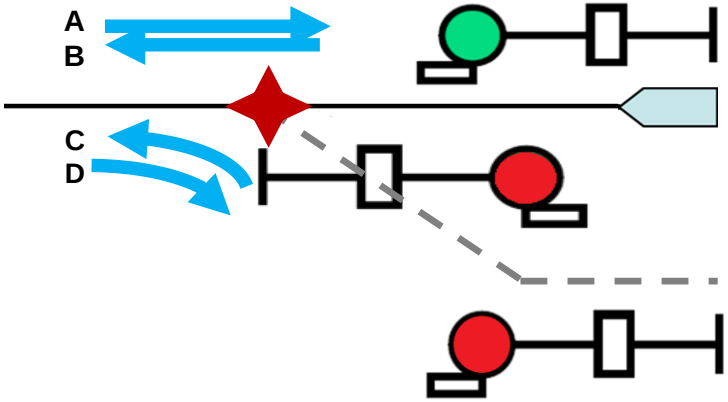
- Bi-directional Traffic Model:
  - Based on the model in the previous step, scale it up to bi-directional case:
    - Direction of a train approaching this point is **completely random (50%, 50%)**
      - In other words, equally sharing the MGT traffic.
    - If the next train is the opposite direction to the previous one: the minimum buffer time should be **increased by 25 minutes.**



  - **Remember to leave room for further development.**
  - Now, what is the simulation output under jamming attack?
    - Generate a sample datasheet, describing each train passing the CP. Example format:
      - Train 0001, 01.07.2019, 03:00 AM, Eastbound, 3500 Tons
      - Train XXXX, 05.26.2019, 05:48 PM, Westbound, 6800 Tons
      - …

Entry Task – Step 3

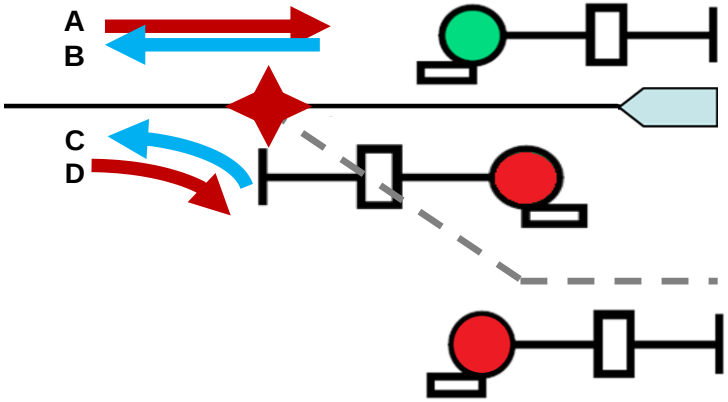
- Diverging Traffic Model:
  - Based on the model in the previous steps, scale it up to a **diverging case**:



- In this case, add an alternate route (dashed line) controlled by the same Control Point, **two more directions (C,D)** of train traffic are introduced.
- Assume four directions equally share the total traffic.
- **(Key point)** Same buffer rules apply, but:
  - Think about **inherent congestions**: how to satisfy buffer rules when two trains, one from C and one from B, arrive within a time slot that close enough?
    E.g. in 5 minutes a C-train and a D-train arrive together.
- Please generate the datasheet describing trains with their individual directions
- Now, what is the estimated traffic under attack?

Bonus Task – Step 4

- Misrouted Model upon Diverging Model:
  - Based on the model in the previous steps, scale it up to a **misroute case**:



- In this case, suppose the DoS attack is no longer our interest.
  Instead, certain Man-in-the-middle attacks would change the dispatchers' signal order message in the wireless link, causing the train goes into the wrong route of the CP.
  Two specific case would happen: A-train goes into D, and D-train goes into A.
- Each case has a same penalty delay as 2 hours to recover (backup the train and start it over) the misrouted train to resume the original route.
  Within this delay, no trains can go through this CP but only wait.
  Upon the previous model you've built, please generate a datasheet with remarks of misrouted train(s).

Final Tips

- Think about the state of train behaviors entering, and leaving the control point, and associated signals.
- Trains only stop and go, and signals only display green and red. Please don’t worry about other trivia, like train speed.
  - However, if you assume anything, please inform us.
- DoS attack and the Man-in-the-middle attacks are just two extremely simplified attacks. The behaviors are narrowed down into the problem descriptions. No other considerations are necessary in this task.
- Review all the tasks as a whole in the beginning for the scalability of your model.

Deliverable

- Choose your favorite method to build up the model.
  - No programming language is specified, but the interface needs to be clear.
- Prepare **a short demonstration** of your model and the simulation results, such as presentation slides, datasheets. Styles are free.
  - Assumptions need to be specifically addressed.
- Inform us the input flexibility of your model so as to change the variables and get a new reasonable output.
- Questions are welcomed before Tuesday (Oct. 30th)'s midnight, and following answers will be sent out by 5 PM Wednesday (Oct. 31st).
- Try your best. Any stage of your work will be considered and evaluated.
- Good luck!