A Generalized Stochastic Petri Net for Survivability and Security Analysis of Intelligent Transportation Systems

Justin L. King
Sahra Sedigh Sarvestani
Ali R. Hurson

Missouri University of Science and Technology

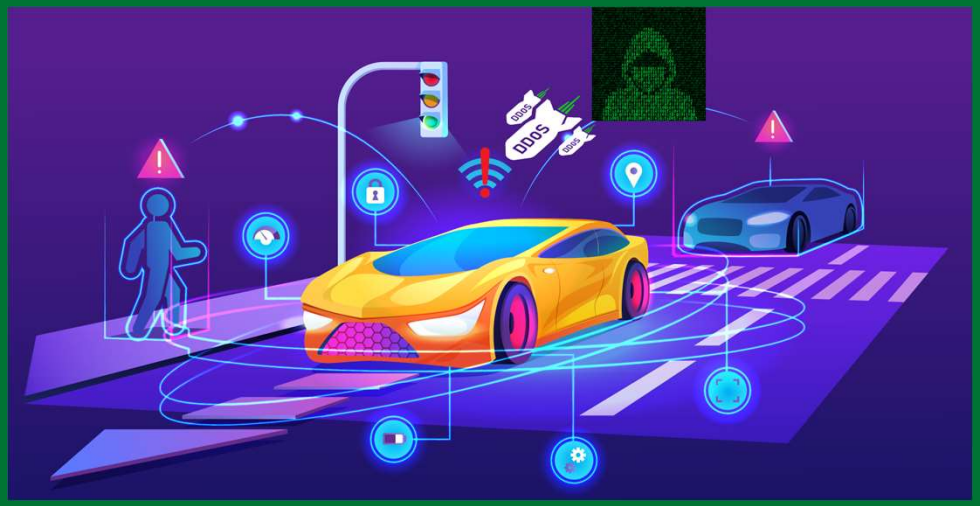
PRESENTER
Sahra Sedigh Sarvestani
sedighs@mst.edu
sites.mst.edu/sendecomp

MOTIVATION

- Connectivity and autonomy increase exposure to cyber attacks
- **Denial-of-service (DoS) attacks** are still a very relevant threat vector to connected autonomous vehicles and the infrastructure of intelligent transportation systems (ITSs)
- **Unavailability of communication, especially in critical windows can affect vehicle survivability**
- Attacks can have **ripple effects** on other vehicles, as well as components connected to intelligent transportation systems
- **Predicting and quantifying the effect of these attacks can guide efforts to fortify communication infrastructure**

METHODS

- We considered the effect of DoS attacks on **802.11p wireless communication** in an ITS
- **More sophisticated attacks exploit the prioritization enabled by Enhanced Distributed Channel Access (EDCA)** to increase the priority of attack messages, resulting in greater harm to legitimate communication
- We used a **generalized stochastic Petri net** to model vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication and predict the effects of these DoS attacks



Denial-of-service attacks against the wireless network can block communication with and by vehicles. Our work **predicts and quantifies** the effect of such attacks on **communication availability** and message failure in an intelligent transportation system.

Download full paper

SIMULATION ENVIRONMENT

- Used to investigate and quantify the effects of attacks, and to **validate the communication failure rates predicted by the model**
- Specific simulators used:
  - **Great SPN**: Discrete-event simulation for Petri net model
  - Vehicles In Network Simulation (**VEINS 5.2**): Customizable simulation model for vehicular networking
  - Simulation of Urban Mobility (**SUMO 1.11.0**): Road traffic simulator; vehicles, maps, pedestrians
  - Objective Modular Network Testbed in C++ (**OMNet++ 5.7**): Event-based network simulator; GUI for information provided by SUMO; data collection alongside VEINS

RESULTS

- We validated our PN model against two different simulation environments, using four types of DoS attacks
- **Our model was 99.9% accurate for "naïve" DoS attacks, and 97% accurate for more sophisticated DoS attacks that exploit prioritized communication**
- A single attacker can block broadcast messages from the roadside unit
- **Communication availability can fall below the 90% threshold** required by IEEE 1609 (Standards for Wireless
- Access in a Vehicular
- Environments (WAVE)
- **Sophisticated attacks can lower communication availability during the critical application window to 0.03%**
- Increasing the number of vehicles or the distance between them exacerbates the effects of DoS attacks against broadcasts
- Future work on this project will investigate the effect of man-in-the-middle attacks on V2V and V2I communication

IEEE IAVVC2024
IEEE International Automated Vehicle Validation Conference
October 21-23, 2024 | Pittsburgh, PA

Funded in part by:
NSF DUE-1742523
NSF DUE-2221559
DEd P200A180095
DEd P200A210121