CRUSER (Consortium for Robotics and Unmanned Systems Education and Research) Faculty and Researchers' Publications

2020

ROS 2 Cyber Network Performance Using Scalable Quality of Service and Security Classifications

Thulasiraman, Preetha

Monterey, California: Naval Postgraduate School

http://hdl.handle.net/10945/65624

ROS 2 Cyber Network Performance Using Scalable Quality of Service and Security Classifications

Network Namespaces

NNS1 — ROS node — Wi-Fi interface
NNS2 — ROS node — Wi-Fi interface
NNS3 — ROS node — Wi-Fi interface
NNS4 — ROS node — Wi-Fi interface
NNS5 — ROS node — Wi-Fi interface

NS-3 Simulated Wi-Fi Network
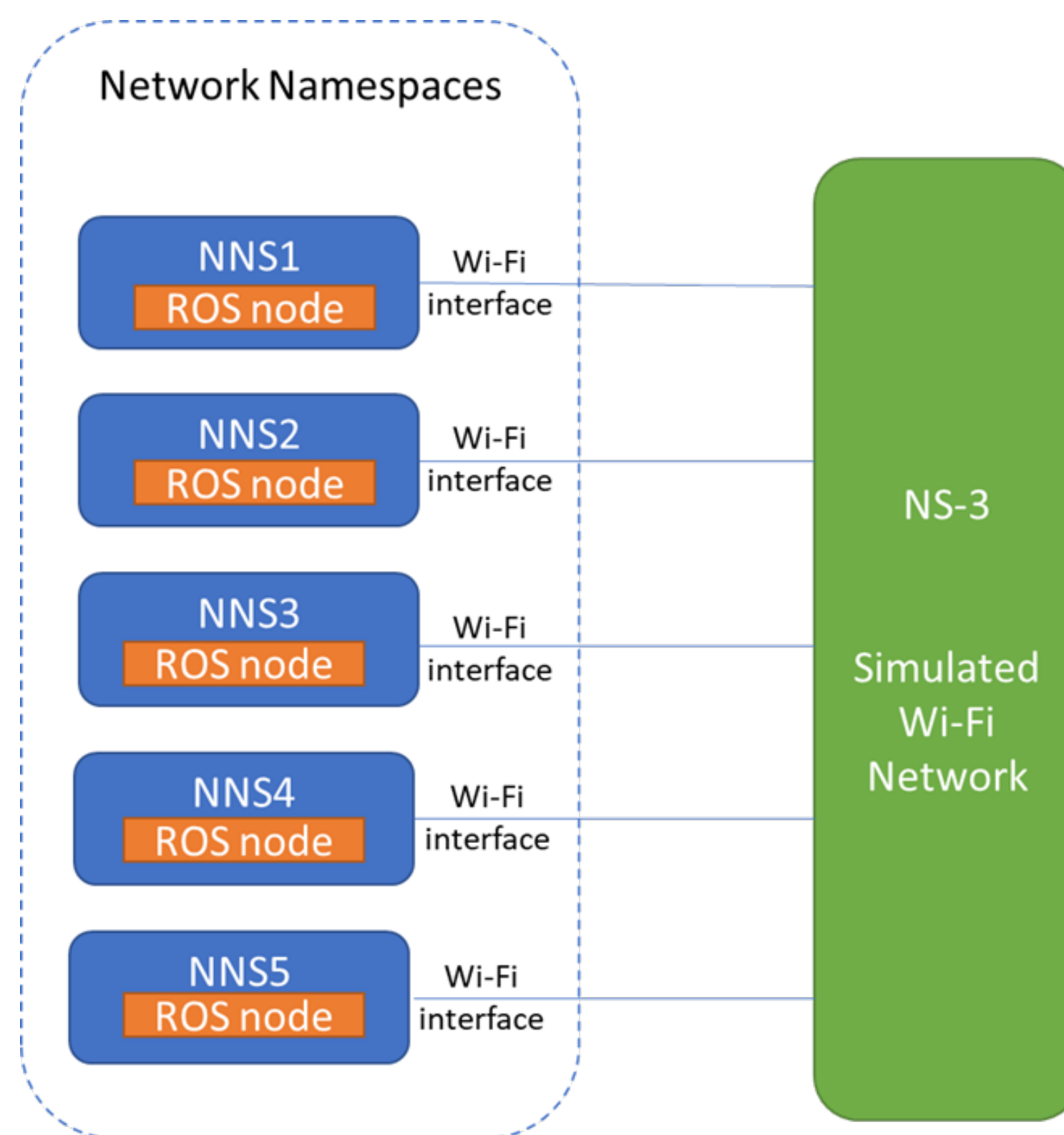
Preliminary simulation architecture with 1 publisher and 4 subscriber ROS 2 nodes communicating over a Wi-Fi network in NS-3. We will build on this architecture to establish more complex use cases.

How

- Use Network Simulator 3 (NS-3) as the primary testing tool for rapid performance evaluation.

- Step 1: Establish functioning NS-3 and ROS 2 simulation setup to include

  - a) Point to point links in which unmanned assets communicate with a ground station over WiFi; b) ad hoc swarm topology in which multiple assets collaborate with one another over WiFi.

  - Analyze performance and tradeoffs. Measurements will include: message latency, overhead, throughput and message loss as a function of network scale.

- Step 2: Study the ROS 2 roadmap to understand how to provide finer control over security configuration settings. Engage with Open Robotics to understand inner workings of ROS 2 security.

What/Deliverables

- Scope of this work is to understand the performance costs associated with Quality of Service (QoS) and security classifications in ROS 2 to align with DoD's Information Assurance (IA) requirements.

- Deliverable 1: Fully functioning ROS 2 use cases for simple (point to point) and complex (ad hoc collaborative) network topologies. Evaluate use cases (in simulation) to quantify how network performance is affected by scale, QoS profiles, and security settings. Provide a written report of findings.

- Deliverable 2: Study fine-tuning security settings for different payloads. ROS 2 roadmap indicates improvements in granularity of security configuration. A report outlining performance guidelines for security plugins on different communication messages will be provided.

- At least one MS EE student thesis in FY20 to support this work.

Why/Objective

- ROS 2 is a critical technology that supports rapid innovation of UxS and can be leveraged for military applications.

- In 2017, OSD identified data transport integration and cybersecurity as two key challenges for UxS.

- Imperative within DoD to ensure IA requirements are met in the context of ROS 2 network performance.

- Simulation as a testing tool allows us to rapidly evaluate performance. A comprehensive set of performance results may help ROS 2 transition to the fleet.

- The proposed research is operationally relevant, in line with the NPS strategic plan and will contribute to relevant thesis study for NPS students

Dr. Preetha Thulasiraman
Department of Electrical and Computer Engineering
pthulas1@nps.edu, Office Ph: 831-656-3456

FY20 Call for Proposals