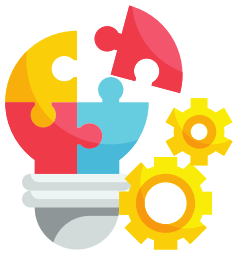
NPS ABSTRACTS

The abstract is like a classified ad for your work. An NPS thesis abstract is no more than 1,500 characters, including spaces (around 200 words).

It should briefly state the background, research problem, purpose, methods, results, and recommendations.

Include these elements:

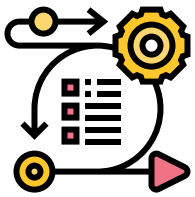


Background & Research Problem

What problem or gap in understanding exists that your research helps address?

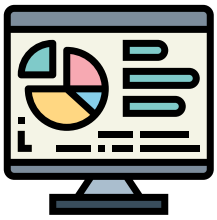
Purpose

What does your research aim to do?



Methods

How did you collect and analyze evidence to answer your research question?



Results

What did you discover? How do your findings help solve the problem?

Recommendations

How can your readers or stakeholders use your research? What comes next?

If using citation-worthy outside information, mention the source in your sentence. Do not use citations.

Source: NPS Thesis Processing Office: What goes in a Thesis Abstract? An Executive Summary?

For more information, see the GWC Abstracts Resource Page or work with a writing coach!

Graduate Writing Center

Trust and Understandability in Autonomous and Unmanned Surface Vehicles

Sample Abstract #1

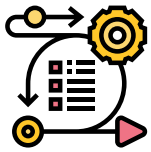
MS in Network Operations and Technology

Within the human-machine relationship, distrust can arise. The Department of Defense utilizes automation, autonomous systems, and artificial intelligence to reduce cognitive workload and improve mission capabilities; however, adoption rates of autonomous unmanned surface vehicles (USVs) remain low. This thesis asks how human distrust of machines and machine learning relates to adoption rates. First, we identify trust components by building upon a model created by Gari Palmer, Anne Selwyn, and Dan Zwillinger in 2016. Then, we identify components that apply to the military environment that could affect the adoption rate such as smoothing time, policies and regulations, competition, robustness, understandability, subjective norm, human interaction, policy effect, risk to force, time sensitivity, war, time between wars, and catastrophic failure. Through S-curve and smoothing modeling, we find that trust components can be quantified in the human machine relationship as positive or negative trust, and that a relationship exists between understandability and adoption. While autonomous system components generally undergo rigorous testing to verify suitability and operability, human-machine trust is not usually incorporated into design and testing phases. When trust is built into the design and acquisition process, adoption of autonomous USVs is more likely to increase. Researchers can apply our trust model to future autonomous systems to mitigate distrust and human-machine teaming.

Background & Research Problem

Purpose

Methods



Results

Recommendations

Kehinde A. Adesanya, Lieutenant Commander, United States Navy
Santhosh K. Shivashankar, Lieutenant Commander, United States Navy

Advisor: Shelley P. Gallup, Department of Information Sciences
Co-Advisor: Douglas J. MacKinnon, Department of Information Sciences

Graduate Writing Center

NPS PRAESTANTIA PER SCIENTIAM 1909

Fingerprinting IPV4 and IPV6 Routers Using ICMP

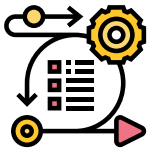
MS in Applied Cyber Operations

Sample Abstract #2

This project reassesses and expands on a simple fingerprinting method for Internet Protocol version 4 (IPv4) routers, and extends that methodology to Internet Protocol version 6 (IPv6) routers. The initial methodology, developed by Vanaubel, Pansiot, Merindol, and Donnet, utilized initial time to live (iTTL) values derived from Internet Control Message Protocol (ICMP) echo-reply and TTL exceeded messages. The current project used ICMP echo-reply and destination unreachable/port unreachable, combined with a third iTTL value derived from ICMP timestamp messages, to strengthen the fingerprint. We adapted the methodology to IPv6-enabled routers using the initial hop limit (iHL) values from ICMPv6 echo-reply and destination unreachable/port unreachable messages. The main goal of this project is to develop a simple fingerprinting technique to identify IPv4 and IPv6 router platforms. We were able to successfully expand the previously developed IPv4 router fingerprint using the ICMP timestamp reply message. Using this fingerprinting methodology, Juniper routers can be identified. However, this fingerprinting technique cannot distinguish between Cisco and Huawei routers. With IPv6, it became evident that most routing devices follow the recommended iHL value of 64 (RFC 1700). Thus, our methodology cannot distinguish between IPv6 routing devices. We recommend additional analysis of Cisco and Huawei devices running IPv4 to identify differences in activity, as well as further research into IPv6 routers.

Background & Research Problem

Methods



Purpose

Results

Recommendations

Fernando Maniego, Chief Petty Officer, United States Navy
Wesley G. Bofman, Chief Petty Officer, United States Navy

Advisor: Robert Beverly, Department of Computer Science
Second Reader: Alan B. Shaffer, Department of Information Sciences

Graduate Writing Center

NPS PRAESTANTIA PER SCIENTIAM 1909

Vision-based Terrain Classification and Learning to Improve Autonomous Ground Vehicle Navigation in Outdoor Environments

Sample Abstract #3

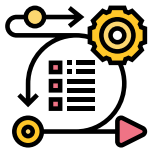
MS in Electrical Engineering

Terrain is an important factor for autonomous ground vehicles (AGV), potentially ruining a mission or the platform itself. The purpose of this thesis is to develop a method for an AGV to identify and avoid hazardous terrain. This work builds on a previously developed system that uses artificial potential fields to avoid obstacles and navigate to a goal. Terrain was identified by developing a random forest machine-learning algorithm, classifying terrain as hazardous or traversable. The random forest was grown using data from images collected during this work. The classification of hazardous terrain was used to generate a repulsive force for use with artificial potential fields. The system was designed to avoid known areas of hazardous terrain using path planning, developing paths using approximate cell decomposition and the A* search algorithm. Tests of the developed random forest revealed accurate classification capabilities for all terrain types, but a tendency to misclassify certain terrain types. Portions of the navigation solution were simulated and confirmed the path planning capability. Trials conducted in a real-world environment revealed the solution stopped the AGV from entering hazardous terrain, and successfully planned routes around hazardous terrain. Improvements to the localization solution will allow the AGV to perform more consistently and over longer ranges.

Background & Research Problem

Purpose

Methods



Results

Recommendations

Caliph Lebrun, Captain, United States Marine Corps

Advisor: Xiaoping Yun, Department of Electrical and Computer Engineering
Second Reader: James Calusdian, Department of Electrical and Computer Engineering

Graduate Writing Center

NPS PRAESTANTIA PER SCIENTIAM 1909