Machine learning and Autonomous System

Safety-Assured Design and Adaptation of Learning-Enabled Autonomous Systems

Definition : It talks about how to keep autonomous systems, like self-driving cars or robots, safe, especially when they use machine learning.

Main points:

- **Challenges in Autonomous Systems:** These systems work in changing and unpredictable environments. It's hard to make sure they are always safe, especially because machine learning (like neural networks) can be difficult to fully understand or predict.
- **A Complete Safety Approach:** The paper suggests looking at safety from all angles, across different parts of the system—like the software, hardware, and different functions (sensing, planning, control, etc.).
- **Connected and Autonomous Vehicles (CAVs):** The document uses CAVs (like self-driving cars) as an example. These vehicles face many uncertainties, like sensor errors or communication problems, which could cause accidents.
- **Machine Learning and Neural Networks:** Machine learning helps with sensing and understanding the environment, but it has weaknesses. For example, small changes in input can trick the system (called adversarial attacks). The document talks about ways to make machine learning models more reliable and safe.
- **Functional and Timing Safety:** It's important not only to make sure the machine learning models work well (functional safety) but also that they do their tasks fast enough (timing safety).
- **Multi-Agent Systems:** Autonomous systems (like cars) can work together to improve safety and performance. However, problems like communication delays can make this difficult.

Integrations between Autonomous Systems and Modern Computing Techniques:

Here are the main points from the review on the integration of autonomous systems with modern computing techniques:

1. **Autonomous Systems Overview**:
   Autonomous systems, which can operate in uncertain environments, originated from control systems. Unlike traditional control systems, they are designed to handle uncertainty without external intervention.
2. **Features of Autonomous Systems**:
   - **Independence**: They can operate without human intervention, saving labor and increasing efficiency.
   - **Wide Operating Range**: They handle environmental uncertainty by broadening their operational capabilities, often integrating subsystems.
   - **Well-Defined Goals**: Their actions are guided by specific goals, prioritizing safety and system objectives.
   - **Adaptation to Uncertainty**: They dynamically adapt to both internal and external changes, with minimal need for outside help.
3. **System Structure**:
   Autonomous systems typically include the following:
   - **Sensors** to gather data from the environment.
   - **Processes** to transform data into actionable outputs.
   - **Models** for decision-making based on environmental input.
   - **Critic Function** to evaluate system performance and improve the model.
   - **Fault Detection** to diagnose and correct internal errors.
4. **Integration with Modern Computing**:
   Autonomous systems can leverage:
   - **Internet of Things (IoT)** for enhanced communication and data gathering from a wide array of devices.
   - **Big Data** to handle large, complex datasets with volume, variety, and velocity challenges.
   - **Federated Learning** to train models across decentralized data sources while preserving privacy.
   - **Over-the-Air (OTA) Technology** for updating system software and models remotely.
5. **Applications**:
   - **Autonomous Vehicles**: These vehicles use sensors like cameras, lidar, and GPS to navigate without human input, potentially reducing traffic accidents.
   - **Health Monitoring**: Autonomous systems can be used for medical applications, such as controlling anesthesia levels during surgery, by using sensors, IoT, and machine learning for real-time decision-making and fault detection.

The paper emphasizes that while these systems are still evolving, they have significant potential for automation in various fields, particularly as they integrate with other advanced technologies.

"Autonomous Systems" by David P. Watson and David H. Scheidt :

Here are the main points from the document "Autonomous Systems" by David P. Watson and David H. Scheidt:

1. **Definition of Autonomous Systems**:
   These are systems that can change their behavior in response to unexpected events without human intervention. They have applications in both civilian and military fields.
2. **Technological Benefits**:
   Autonomous systems offer significant cost reductions and risk mitigation. They can operate in environments where direct human control is impossible, making them transformative in areas such as space exploration and deep-sea operations.
3. **History**:
   Autonomous systems' roots trace back to early attempts at automata and evolved through cybernetics in the 1940s, where Norbert Wiener developed the feedback control theory. Modern autonomous systems began to take shape with digital control electronics in the 1970s.
4. **Application Domains**:
   - **Maritime**: Focused on unmanned underwater vehicles (UUVs) for surveillance and mine countermeasures.
   - **Ground**: Challenges include the complexity of navigating terrestrial environments, with research on semi-autonomous mobility and control.
   - **Air**: UAV (Unmanned Aerial Vehicle) systems are being developed for military applications, such as the J-UCAS program for combat missions.
   - **Space**: Space missions, especially deep-space missions, require high-level autonomy due to communication delays, requiring onboard decision-making.
5. **Critical Technologies**:
   - **Planning and Scheduling**: Autonomous systems must establish and adjust plans in real-time, even under changing conditions.
   - **Layered Control**: This architecture allows systems to handle events at different timescales, balancing responsiveness and robustness.
   - **Model-Based Reasoning**: Autonomous systems use models to estimate system states and make decisions, rather than relying on predefined rule sets.
   - **Reactive Behavior**: Systems use real-time control loops to maintain stability, with higher-level reasoning for more complex decisions.
   - **Behavior Coordination**: Swarm intelligence and distributed control are key research areas, especially for coordinating multiple autonomous systems toward a common goal.
6. **Research Challenges**:
   The document identifies several challenges, including improving learning capabilities, handling complex mission plans, and ensuring robustness in the face of unanticipated events. Additionally, autonomy must be verifiable and reliable, especially in mission-critical scenarios like space exploration.
7. **Future of Autonomous Systems**:
   The advancement of autonomy will depend on overcoming technological challenges

related to sensing, perception, control, and communication. The goal is to create systems that can operate independently while adapting to dynamic environments.

Revealing the Autonomous System Taxonomy: The Machine Learning Approach

Here are the main points from the paper *"Revealing the Autonomous System Taxonomy: The Machine Learning Approach"* by Xenofontas Dimitropoulos et al.:

1. **Autonomous Systems (AS) in the Internet**:
   Autonomous Systems are independently managed networks that together make up the global Internet. There are over 20,000 AS identifiers, representing different types of organizations like ISPs, universities, and private companies.
2. **Challenges in Modeling AS Topology**:
   The rapid growth and diversity of ASes make it difficult to model the Internet accurately. Different types of ASes, such as large ISPs or small businesses, have vastly different network characteristics and growth patterns. This diversity complicates attempts to map the Internet infrastructure.
3. **Need for AS Classification**:
   Understanding the types of ASes is crucial for realistic Internet modeling. AS classification helps identify network evolution patterns, improve Internet simulations, and distinguish between different types of users (e.g., home vs. business).
4. **Machine Learning for AS Classification**:
   The paper introduces a novel machine learning-based approach to classify ASes into six categories: Large ISPs, Small ISPs, Customer ASes, Universities, Internet Exchange Points (IXPs), and Network Information Centers (NICs). Using data from the Internet Routing Registries (IRR) and BGP tables, the researchers create a classification algorithm with a 78.1% accuracy rate.
5. **Attributes Used for Classification**:
   The researchers collect six key attributes from the AS data:
   - **Organization description** (e.g., name, function)
   - **Number of customers**
   - **Number of providers**
   - **Number of peers**
   - **Number of advertised IP prefixes**
   - **Equivalent number of /24 IP prefixes** (to reflect network size)
6. **Results**:
   The machine learning algorithm accurately classifies the majority of ASes. 63% are Customer ASes, 30.1% are Small ISPs, 4.7% are Universities, and 0.2% are Large ISPs or IXPs.
7. **Significance of the Study**:
   The research provides a better understanding of the structure and evolution of the Internet by offering a detailed taxonomy of ASes. This taxonomy can improve Internet

simulations and modeling, particularly in terms of routing policies and network infrastructure.

8. **Public Dataset Release**:
   The researchers release the AS classification dataset, which includes detailed information on each AS's type, business relationships, and IP space usage, encouraging further research into Internet topology.

This study contributes to a more accurate representation of Internet infrastructure and offers tools for future research in network analysis and Internet evolution.