Formal Methods Enhance Deep Learning for Smart Cities:

Challenges and future directions

Rigorous approaches based on formal methods have the potential to fundamentally improve many aspects of deep learning. This article discusses the challenges and future directions of formal methods enhanced deep learning for smart cities.

By Meiyi Ma

DOI: 10.1145/3522694

As artificial intelligence (AI) technologies advance, deep learning has been broadly applied to cyber-physical systems (CPS) and the internet of things (IoT), which form the basis of emerging and future services in smart cities. Furthermore, the development of faster and more reliable networks, especially with the extensive deployment of 5G, is accelerating the integration of smart city services.

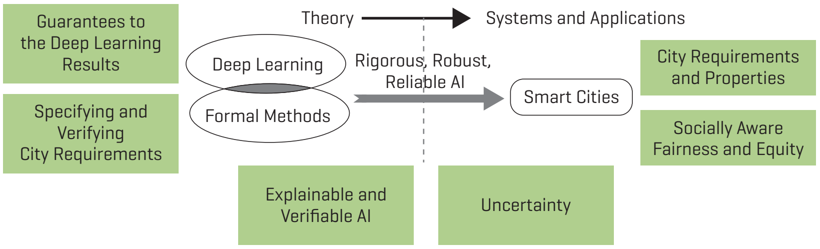
But while significant research efforts have been made toward building smarter services, sensors, and infrastructures in cities, the research challenge of ensuring that real-time operations satisfy safety and performance requirements has received only scant attention.

First, most services are developed independently by different stakeholders within their own contexts. Integrating multiple CPS into the same environment could cause problems like conflicts among their actions that are not foreseen during the design process. For instance, a congestion control service may change a traffic light system to improve traffic due to a football game, whereas an environmental control service may change the same traffic light system due to noise and pollution emissions. As a result, there might arise: 1) a direct conflict between these two services or with a third service, for example, an ambulance is delayed due to conflicting traffic light schedules; or 2) an environmental conflict with another service, for example, a power plants' emissions control service is not aware of increased pollutant emissions due to an unexpected increase in traffic and thus does not update their emission setting, which ultimately leads to the combined emissions violating emission standards. Such conflicts could lead to serious consequences and adversely impact millions of lives every day, for example, in the form of delayed travel time, hazardous air pollution levels, or compromised pedestrian safety. The question of how we might build reliable integrated smart cities—despite facing significant new challenges due to the increased integration, complexity, and environmental uncertainties—becomes a central problem.

Moreover, many services are supported by deep learning models. However current deep learning techniques are not mature enough to deal with the challenges—safety-critical, large-scale services that operate in highly uncertain settings, with humans in the loop. One of the key reasons is that, as data-driven approaches, they

Image by Andrij Borys Associates, using Shutterstock

Figure 1. Formal methods enhanced deep learning for smart cities.


Guarantees to the Deep Learning Results
Specifying and Verifying City Requirements
Theory
Systems and Applications
Deep Learning
Formal Methods
Rigorous, Robust, Reliable AI
Smart Cities
City Requirements and Properties
Socially Aware Fairness and Equity
Explainable and Verifiable AI
Uncertainty

often do not consider system properties, environmental requirements, or the complex interactions with other services or humans in the same environment. Their reliability when deployed in real-world environments then becomes questionable.

Toward building robust and reliable AI for smart cities, researchers have proposed that rigorous approaches based on formal methods have the potential to fundamentally improve many aspects of deep learning, including transparency, robustness, algorithmic equity, and fairness, among others [1]. As mathematically rigorous techniques, formal methods have been widely applied to verifying and evaluating critical systems such as autonomous aircraft technology. This motivates a novel research direction of verifying machine learning using formal methods in recent years, mainly targeting applications with well-specified safety requirements such as autonomous driving and robotics. However, verification is only meaningful when paired with high-quality formal specifications. The problem with current approaches is that such specification does not exist or is highly under-explored in smart cities. This poses great challenges to applying formal methods to machine learning in a smart city context.

We, therefore, present a novel research direction—developing rigorous and robust AI for smart cities by integrating formal methods and deep learning. We first discuss the characteristics of smart city services. Next, we present the research challenges and future directions in developing formal methods enhanced deep learning for smart cities. Specifically, as shown in Figure 1, we focus on addressing six research questions. How can we guarantee that deep learning results will satisfy system properties? How can city requirements and properties be identified from large-scale city data? How do we specify and verify city requirements? How should uncertainty be dealt with in smart cities? How can we develop explainable and verifiable AI methods for smart cities? How do we enhance socially aware equity and fairness in smart cities?

CHARACTERISTICS OF SMART CITY SERVICES

The characteristics of a smart city service describe how it interacts with the city's resources and other services, and how it affects the environment and the humans living in it. Some fundamental characteristics of smart city services and their interactions with one another have been introduced in our previous work [2]. Here we restate them in the context of applying formal methods enhanced deep learning techniques.

Uncertainty. There are usually three types of uncertainty in the city applications: data, model, and event/behavior uncertainty. The first two types also broadly exist in many other applications and have been extensively studied in deep learning. The third one refers to unforeseen events or processes that cannot be accounted for by the services ahead of time or are unknown to the service, but affect its performance. Uncertainty can occur in the different layers of a service: sensing layer (a vehicle-attached pollution sensor moved from its expected location), communication layer (network failure), or actuation layer (control valve only opens partially). The uncertainty poses considerable challenges for building accurate deep learning models and raises demands for guarantees from these models.

Dynamism. While some services operate with a static schedule (for example, sending out school buses to pick up students each morning), a major portion of services function dynamically. For example, a public transport service schedules bus routes and frequency based on demand—planning for more buses when there are large events like festivals. Such dynamic operations can introduce complexity if the service shares resources (sensors/actuators/data) with other services. Moreover, city data can barely capture such complex dynamism. How can we inject extra city knowledge on the dynamism into learning models?

Real time. In a smart city, decision-makers and services frequently rely on real-time information for operational decision-making. For example, emergency response services send fire trucks and ambulances when an accident is detected or reported. Timing is critical in such scenarios. Moreover, suppose a service can predict the likelihood of an incident and reallocate the resources accordingly. In that case, it will save a large amount of response time or even prevent the incident from happening. Therefore, there is a high demand for efficient predictive monitoring in real time.

Efficiency. Efficiency can be measured as a function of resources, cost, and time. Maximizing efficiency for one service can often lead to resource constraints for another service if the two services share any resources. Thus, it poses an optimization problem with constraints on resources and operational costs. On the other hand, it also indicates a high demand for efficiency on the services' models. However, formal verification for large-scale problems tends to be very costly. Developing an effective and efficient verified learning algorithm is an open research question.

Ownership. Services are developed by different stakeholders. A service can be private, public, or commercial in terms of ownership. The degree of interaction and information flow between services with different ownerships can vary according to service design and city policies. Meanwhile, building safe and secure interactions between services and city operating centers become a critical step toward an integrated smart city system.

Although not completely, these characteristics outline the potential complexity of smart city services. Targeting the demands raised by city characteristics, we will now discuss the challenges and future directions of developing formal methods enhanced deep learning for smart cities.

PROVIDING GUARANTEES TO DEEP LEARNING RESULTS

Deep learning models have outstanding capabilities for prediction and decision-making support for smart services in smart cities. However, in large-scale and complex integrated systems like smart cities, deep learning models are not always robust, and are often subject to anomalies and uncertainty. Systems in cities often follow certain model properties, however, they cannot be guaranteed by existing prediction models. Therefore, guaranteeing that deep learning results will satisfy system properties becomes an important research question. In previous work, we developed a formal logic enhanced learning framework that implements logic-based criteria to enhance recurrent neural network (RNN) models to follow system critical properties [3]. The framework incorporates critical properties into the learning process in an end-to-end manner with backpropagation. It is general and can be applied to various RNN models. It was evaluated on large-scale real-world city datasets, which showed the new framework not only improves the accuracy of predictions in various RNN models, but also guarantees the satisfaction of model properties and increases the robustness of RNNs.

IDENTIFYING CITY REQUIREMENTS AND PROPERTIES

An important step in bringing integrated formal methods and machine learning techniques to real-world applications is systematically learning from large-scale real-world data and applications. However, unlike areas of robotics and autonomous driving where specifications have been extensively studied, requirements and properties are extremely underexploited in smart cities. This poses significant challenges to incorporating formal methods into smart city models. In the current state-of-the-art approach, researchers conducted a series of data-driven analytics. To identify desirable features to have in a specification language for cities, we systematically studied and annotated more than a thousand city requirements (for example, standards and regulations) across different domains—including energy, environment, transportation and public safety—from more than 80 cities around the world [4]. We also identified types of service conflicts, model properties, and uncertainty by analyzing cross-domain city data [5, 6]. However, the scalability and generalizability of these studies are still insufficient. Furthermore, systematically identifying and mining real-world city specifications from a noisy and complex city environment with support from city experts and citizens in the loop is a promising yet challenging research question.

The research challenge of ensuring that real-time operations satisfy safety and performance requirements has received only scant attention.

SPECIFYING AND VERIFYING CITY REQUIREMENTS

To introduce city requirements into deep learning models, a key question is whether large-scale city-states satisfy a wide range of system requirements at runtime. The challenges here include how an expressive formal language can be used to specify system requirements, so that they can be understood by machines, and how to efficiently monitor requirements that may involve multiple sensor data streams (for example, some requirements are concerned with thousands of sensors in a smart city). Safety requirements in smart cities are specified in natural language, which is often inaccurate and ambiguous. Therefore, it is difficult for machines to understand and verify the requirements. In addition, the city-states (data) are large-scale and heterogeneous across spatial and temporal domains, which raises great challenges for real-time monitoring. Existing formal languages (for example, STL and its extensions [7]) are insufficient for specifying the complex spatial-temporal requirements and inefficient for monitoring large-scale signals in real time. To bring formal logic to solve real-world problems, researchers have developed novel formal specification languages (for example, SaSTL [4] and STL-U [6]) and new efficient monitoring algorithms. This logic is powerful and can verify realistic requirements based on time, space, aggregation, and uncertainty. From formalizing 1,000 real city requirements the results show SaSTL-U has a much higher coverage expressiveness (95%) than the state of the art. In future work, with the increasing number of smart services in cities, developing scalable methods for checking the correctness and security of city operation with runtime assurance focusing on quantitative properties (for example, uncertainty quantification, and probabilities) is of great importance.

DEALING WITH UNCERTAINTY

As one of the key characteristics of smart services in cities, uncertainty significantly affects the performance of deep learning models. How can we predict a system's future states and check if the prediction satisfies system requirements? With such capability, the system operator may take actions in advance to prevent predicted future requirement violations. A key challenge of predictive monitoring is accounting for the inherent uncertainty (for example, due to sensor and environmental noise, unexpected events, accidents, or human behaviors) in the city. We developed a novel approach for monitoring sequential predictions generated from Bayesian recurrent neural networks that can capture the inherent uncertainty in CPS, drawing on insights from our study of real-world city datasets [6]. We also developed novel criteria that leverage STL-U monitoring results to calibrate the uncertainty estimation in Bayesian RNNs. Evaluation results on large-scale real-world city data show these approaches improve the accuracy and robustness of deep learning models and achieve well-calibrated uncertainty. Moreover, the system also effectively improves smart cities' safety and performance in smart city simulations.

DEVELOPING EXPLAINABLE AND VERIFIABLE AI METHODS FOR SMART CITIES

Despite the impressive achievements of machine learning in real-world applications, explainability is still one of the biggest concerns of applying AI models to safety-critical CPS/IoT. Rigorous approaches based on formal methods have the potential to fundamentally conquer this limitation by verifying and guiding deep learning models. Researchers have developed learning frameworks by incorporating formal verification and synthesis techniques. Potential future directions include formally verifying the results to detect adversarial and out-of-distribution inputs, verifying the intermediate learning process with hyper-properties, formal knowledge distillation, uncertainty quantification, logic-based learning criteria, among others.

ENHANCING SOCIALLY AWARE EQUITY AND FAIRNESS

Human beings (as citizens and city decision-makers) play essential roles in smart cities. Socially aware equity and fairness in smart city systems is another key direction that researchers have been exploring in recent years. Increasing integration of smart cities (for example, city services and their stakeholders, as well as decision-makers from different departments and agencies) unavoidably adds more challenges in maintaining socially aware equity and fairness in smart cities. Following previous work on conflict detection and resolution among city services [8, 9], one direction could be addressing human-in-the-loop conflicts such as conflicting human physiology (for example, increasing and decreasing glucose levels by two healthcare services at the same time) and conflicts between human decisions or policies. For different application domains, the definition and measurement of fairness are very different. This motivates the development of customizable and more sophisticated measurements and criteria to train the algorithms. Formal specification and verification techniques are effective ways to fulfill this gap. For example, applying formal methods to measure and validate specifications regarding socially aware fairness, accountability, transparency, and trade-offs in smart services is still an under-exploited direction.

References

[1] Ma, M. *Formal Methods Enhanced Deep Learning for Integrated Cyber-Physical Systems.* Ph.D. dissertation. University of Virginia, 2021.

[2] Ma, M., Preum, S. M., Tarneberg, W., Ahmed, M., Ruiters, M., and Stankovic, J. Detection of runtime conflicts among services in smart cities. In *Proceedings of the 2016 IEEE International Conference on Smart Computing* (SMARTCOMP). IEEE, 2016.

[3] Ma, M., Gao, J., Feng, L., and Stankovic, J. STLnet: Signal temporal logic enforced multivariate recurrent neural networks. In *Advances in Neural Information Processing Systems (NeurIPS).* 33, 2020.

[4] Ma, M., Bartocci, E., Lifland, Stankovic, J., and Feng, L. A novel spatial temporal specification-based monitoring system for smart cities. *IEEE Internet of Things Journal* 8, 15 (2021), 11793–11806.

[5] Ma, M., Preum, S. M., Ahmed, M. Y., Tärneberg, W., Hendawi, A., and Stankovic, J. A. Data sets, modeling, and decision making in smart cities: A survey. *ACM Transactions on Cyber-Physical Systems* 4, 2 (2019), 1–28.

[6] Ma, M., Stankovic, J., Bartocci, E., and Feng, L. Predictive monitoring with logic calibrated uncertainty for cyber-physical systems. *ACM Transactions on Embedded Computing Systems (TECS)* 20, 5s (2021).

[7] Bartocci, E., Deshmukh, J., Donzé, A., Fainekos, G., Maler, O., Ničković, and Sankaranarayanan, S. Specification-based monitoring of cyber physical systems: A survey on theory, tools and applications. In *Lectures on Runtime Verification*, Springer, Cham, 2018, 135–175.

[8] Ma, M., Preum, S. M., and Stankovic, J. A. Cityguard: A watchdog for safety aware conflict detection in smart cities. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation.* ACM, New York, 2017, 259–270.

[9] Ma, M., Stankovic, J. A., and Feng, L. CityResolver: A decision support system for conflict resolution in smart cities. In *Proceedings of the 2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems* (ICCPS). ACM, New York, 2018, 55–64.

Biography

Meiyi Ma is an assistant professor in the Department of Computer Science at Vanderbilt University. Her research interests include cyber-physical systems, deep learning, and formal methods with applications in areas of smart cities and healthcare. Ma received a Ph.D. in computer science from the University of Virginia.