Challenges and Directions for Ambient Intelligence: A Cyber Physical Systems Perspective

John A. Stankovic
Computer Science
University of Virginia
Charlottesville, USA
stankovic@virginia.edu

Meiyi Ma
Computer Science
Vanderbilt University
Nashville, USA
meiyi.ma@vanderbilt.edu

Sarah Masud Preum
Computer Science
Dartmouth College
Hanover, USA
sarah.masud.preum@dartmouth.edu

Homa Alemzadeh
Electrical and Computer Eng.
University of Virginia
Charlottesville, USA
ha4d@virginia.edu

2021 IEEE Third International Conference on Cognitive Machine Intelligence (CogMI) | 978-1-6654-1621-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/COGMI52975.2021.00038

***Abstract*—Sensing is becoming more and more pervasive. New sensing modalities are enabling the collection of data not previously available. Artificial Intelligence (AI) and cognitive assistance technologies are improving rapidly. Cyber Physical Systems (CPS) are making significant progress in utilizing AI and Machine Learning (ML). This confluence of technologies is giving rise to the potential to achieve the vision of ambient intelligence. This paper describes some of the main challenges and research directions for ambient intelligence from a CPS perspective.**

***Index Terms*—Ambient Intelligence, Cyber Physical Systems, Cognitive Assistance, Intelligent Systems**

I. Introduction

Cyber Physical Systems (CPS) research is building solutions to support complex systems that are often safety critical. This includes smart cities, smart health, autonomous systems, robotic surgery, support for first responders and many others. Many of the current solutions and future research directions include the use of Artificial Intelligence (AI), including cognitive assistance. However, currently the level of cognitive assistance is sometimes relatively simple or focused on a very specific task or individual [1]. It is expected that future systems will continue to enhance and generalize cognitive assistance to work together with and support an infrastructure of ambient intelligence. Ambient intelligence has many definitions [2], [3], but we envision it as a seamless infrastructure that integrates in-body, on-body, in-situ sensors, actuators, and interacting cognitive assistants. As an example, for Smart Health this may include in-body heart and insulin pumps, on body devices that measure multiple physiological parameters, access to medical records and medications, in-home smart devices that monitor and aid with activities of daily living, in-situ devices in the environment that provide information about air pollution, temperature, flu and covid rates in a location, etc., and associated services that exchange data and knowledge among these modalities in order to have a holistic health view of the person and to provide ambient intelligence to improve health [4]. In many cases ambient intelligence may have safety critical implications. Therefore, it is imperative that CPS technology be merged with AI to address many of the future research challenges.

This paper was supported, in part, by the National Science Foundation NRT program under Grant 1829004, the award 60NANB17D162 from the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), and a research grant from the Commonwealth Cyber Initiative (CCI).

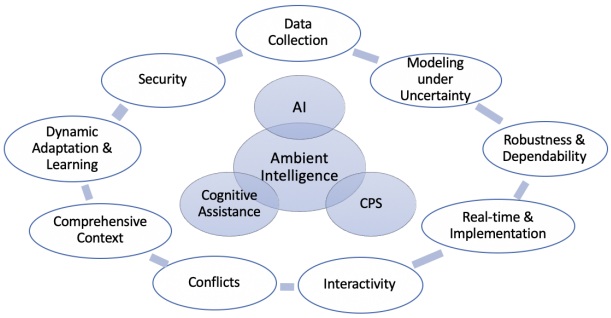

Fig. 1. Challenges and Directions for Ambient Intelligence

This paper highlights the research challenges for merging CPS and AI to achieve ambient intelligence by discussing the following areas: data collection, modeling under uncertainty, robustness and dependability, real-time and implementation issues, interactivity, conflicts, comprehensive context, dynamic adaptation and learning, and security. Overall, we articulate challenges, demonstrate that CPS is an essential component for solving many of these challenges, and, when known, highlight some current research that show significant promise. The areas discussed are meant to be representative and, therefore, not complete. See Figure 1.

II. Overview of Cognitive Assistance, Ambient Intelligence, and CPS

The focus of cognitive assistance is on integrating AI with cognitive processes and humans processes and actions. The focus of ambient intelligence is on the physical environment interactions with humans and AI. CPS focuse on the intersection of the cyber with the physical environment. Hence, these three areas of research significantly overlap. In this section we provide a brief background on each of these areas as a basis for the remaining sections of the paper.

A. Overview of Cognitive Assistants

Cognitive Assistants are envisioned to complement human capabilities rather than replace human capabilities [5], [6]. A cognitive assistant is a program that augments human

978-1-6654-1621-4/21/$31.00 ©2021 IEEE
DOI 10.1109/CogMI52975.2021.00038

intelligence by offering complementary cognitive capabilities to a human [6]. Cognitive assistants are also referred to as cognitive agents [7]. Cognitive assistants are capable of performing time-consuming, daunting or computationally demanding cognitive tasks in which a machine achieves higher efficiency and accuracy than a human. Some of the defining characteristics of cognitive assistants are interactivity, context-awareness, and adaptive learning [1], [7], [8]. Ideally, cognitive assistants maintain an explicit model of the environment, have one or more goals to be accomplished, perceive external events, make plans to change the world taking into account their goals, and finally implement them by acting upon the environment [7]. Additional definitions of cognitive assistants can be found in [1].

Existing cognitive assistants have a wide variety of modes of interaction including verbal and non-verbal interaction. These interactions are often reactive (i.e., triggered by an event) rather than proactive. Existing cognitive assistants react differently according to different contexts, e.g., Google map reminds the user if the target destination will be closed by the expected time of arrival and thus provides spatio-temporal context-aware interaction. Some cognitive assistants support users' personal contexts (including physiological, psychological, behavioral contexts) and situational contexts (e.g., the Google assistant referring to inclement weather as the user asks about a outdoor calendar event). Currently, contexts are encoded in the underlying system of a cognitive assistant and it identifies the context based on user interaction or situational awareness. While cognitive assistants have made a lot of progress in identifying context and provide context-aware interaction for different applications, there are still a lot of challenges for adaptive learning. Specifically, existing cognitive assistants still lack maturity in identifying and characterizing dynamic environments and user behavior, resolving ambiguity, tolerating unpredictability, and distinguishing between signal and noise in past interactions. Ambient intelligence might help to bridge this gap.

B. Overview of Ambient Intelligence

Ambient intelligence refers to the use of ubiquitous smart devices and AI such that physical environments interact intelligently and unobtrusively with people (see Figure 2). Ambient intelligence should account for peoples' conditions and needs, and provide services to people with customized responses. The environments are diverse and include homes, work, hospitals, schools, and cities. The services can be extremely broad and can involve healthcare, daily life activities, work support, and entertainment.

The underlying technologies required to support ambient intelligence include: monitoring and interpreting the environment's and user's state, representing and dynamically updating the information and knowledge associated with the environment, perform modeling and simulating or analyzing entities in the environment, making decisions, taking actions, continual learning about the environment and people, and interacting with humans unobtrusively and with privacy, security and safety guarantees.

Some question and answer systems and systems like Alexa and Siri are sometimes considered as taking steps towards ambient intelligence, But these systems tend to have limited intelligence and may not use environment or user based sensors to provide significant contextual understanding as a basis for (more) intelligent services. Many challenges remain to be solved before we achieve ambient intelligence. Some of these challenges are discussed in this paper.

C. Overview of CPS

Many CPS are quite complicated and benefit from Machine Learning (ML) and AI. Consequently, any advances in ML and AI can substantially benefit CPS. Alternatively, CPS technology provides capabilities that can support ML and AI tasks such as cognitive assistance and ambient intelligence. What are these CPS technologies?

In most CPS, requirements are carefully stated in a formal language. Perhaps ambient intelligence can benefit from formal specifications. Today, it is rare to see a ML or AI solution carefully state the requirements that must be met by the solution. CPS also address issues such as real-time, safety criticalness, uncertainties, guarantees, and control; all topics that can improve cognitive assistance and ambient intelligence. For example, often a cognitive assistant must recognize the context of a user via sensors and then decide on an intervention, in time. Real-time scheduling and resource assignment solutions from CPS can be applied to a cognitive assistant.

A cognitive assistant must also be very careful with respect to recommended actions or interventions and can often take actions that are safety critical. Applying safety critical technology such as robustness techniques, redundancy, code verification and others can improve a cognitive assistant use in practice. Uncertainties are rampant in ambient intelligence environments due to many factors including environment and human dynamics. Representing uncertainties and providing associated guarantees are necessary. CPS have a rich set of techniques to model uncertainties and map these to, at least, probabilistic guarantees. Of course, ML and AI also often address uncertainties and integrating ideas from the two communities would be beneficial to both.

A main component of most CPS is feedback control. A rich literature exists for controlling systems to meet performance requirements including stability. Control theory also utilizes careful methodologies to create solutions. Applying these methodologies and other concepts, e.g., passivity, can improve the performance of a cognitive assistant by providing, with new research, carefully defined properties that one can expect the cognitive assistant to follow. There is also a close relationship between reinforcement learning and control theory.

In the remainder of this paper we address other issues where CPS, cognitive assistance and ambient intelligence can be mutually beneficial.

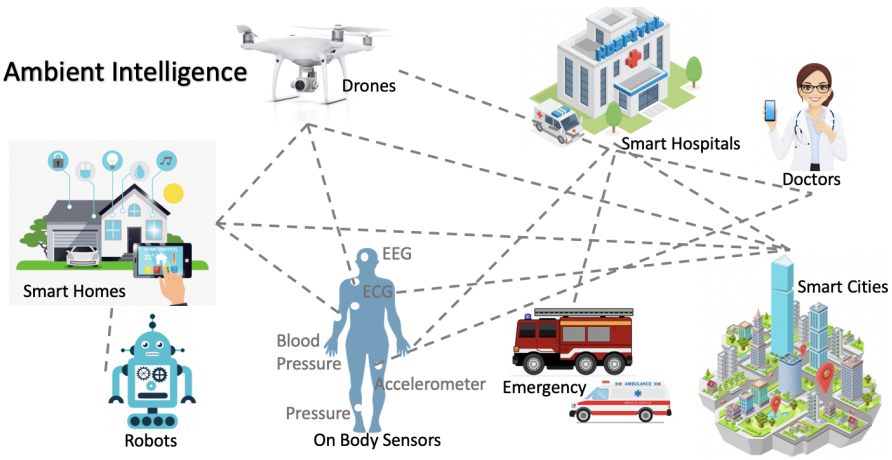

Fig. 2. Ambient Intelligence

III. Data Collection

Data collection is critical for effective ambient intelligence. Since ambient intelligent systems are expected to interact with dynamic user behavior and complex environments, ideally they require life long learning [9]. There are two aspect of data collection for ambient intelligence: CPS-related and AI or ML related.

A. Data Collection Challenges and Opportunities for CPS

Existing cognitive assistants utilize a wide array of sensors for data collection, including (i) primitive sensors, (ii) physiological sensors, (iii) acoustic and ultrasonic sensors, (iv) RGB cameras, (v) RGB-D and depth sensors, and (vi) GPS and Bluetooth low energy (BLE) beacons. Primitive sensors are used to sense the environment and users interactions with the environment, such as, PIR motion detectors, temperature sensors, contact sensors, light sensors, and humidity sensors. Physiological sensors are used to measure and track changes in physiological states of an user, e.g., skin conductance sensors to track emotion or mood of an user, pulse oximeter to measure oxygen saturation, or a blood glucose monitor to detect if a diabetic patient is at risk.

The major CPS challenge is collecting real world data continuously and reliably as this affects the accuracy of decisions made by ambient intelligence. Data collection is difficult for several reasons, including but not limited to in-body, on-body, in-situ sensor failure, disruption in sensor networks [10], sensor maintenance, and data aggregation in the cloud. Using multimodal sensor fusion can be helpful to collect relevant ambient data and maintain some data redundancy. For instance, collecting both depth sensor data and IMU sensor data to keep track of user motion for indoor navigational assistance. CPS solutions should be enhanced to characterize missing data. For instance, user activity monitoring and tracking often suffer from missing data. Such missing data can be attributed to a variety of factors including device failures, system bugs, local network connection failures, cloud errors, and battery failures.

B. Data Collection Challenges and Opportunities for ML

Another aspect of data collection is collecting the right data for training a machine learning model to produce the target inference, e.g., recognizing a user's command, or other interaction, tracking user activity, or detecting a change in a user's behavior. From the ML perspective the major challenges in data collection are collecting the required amount of data for training, obtaining realistic and comprehensive training data that covers all expected future scenarios, and dealing with missing data.

Ambient intelligent systems are expected to continually learn from past data. However, the amount of available data is often limited and data annotation might be challenging especially for log lived and adaptive situations. Inspired from the domain of NLP and computer vision, ambient intelligent system can integrate transfer learning, weak supervision, and meta learning based solutions to address the challenge of low training data and limited annotation. For domain specific problems with limited data and annotation, another potential solution is knowledge integration with a specialized lexicon or vocabulary [11], [12].

Intelligent systems often suffer from skewed training datasets where there is more data from general or regular cases, but fewer or none from corner cases, outliers, or rare situations. For instance, for voice activated ambient intelligence the speech recognition models can be trained on vast amount of native speakers' audio data and data without significant background noise. However, the trained model might not generalize to users who are not native English speakers, or situations where there is a lot of background noise [11]. Another challenge is that the dynamic environment and user interactions might generate new data such that the original static training dataset is no longer representative of the new test data. Lifelong learning can be effective in such cases [9]. Also, in safety-critical cases (e.g., robotic surgery, medical devices, aircraft or autonomous vehicle navigation) identifying and characterizing 'rare event' cases are critical so that the

intelligent system does not commit fatal or serious mistakes.

IV. Modeling Under Uncertainty

Ambient intelligence often predicts the future states of the system, environment or human in the loop, and checks if the prediction satisfies its requirements. With this capability, cognitive assistance may take actions in advance to prevent such predicted future requirement violations. Due to the dynamics of environments, a key challenge of predictive monitoring is how to account for the inherent uncertainty (e.g., due to sensor and environmental noise, unexpected events, accidents, and individual personal behaviors) in the environment. Therefore, it is necessary for ambient intelligence to model with uncertainty.

Deep learning techniques have been increasingly applied to predict system and environment states (e.g., glucose level forecasting) for ambient intelligence. However, previous works mostly focus on generating predictions only and rarely account for the uncertainty inherent in the environment. Recent advances such as Bayesian deep learning techniques can adapt the prediction output stochastically as a sequence of posterior probability distributions over a finite discrete-time domain. Variational inference and Monte Carlo Dropout [13], [14] are two common approaches to perform an approximated inference on Bayesian Neural Networks. The first one builds Bayesian Neural Networks [15] to represent a probabilistic model that infers a distribution as output. However, the complexity of inference prevents the prevalence of the model in practice. By exploiting the dropout structure in a deep neural network, these approaches turn the original Neural Network model into a simple Bayesian Neural Network without changing the structure and apply approximated inference with the Monte Carlo approach. Existing works [14], [16], [17] mostly focus uncertain estimation on single-time classification or regression tasks. Moreover, existing methods often use the loss functions of deep learning models (e.g., mean square error, negative log-likelihood, KL divergence) as the only metrics for the uncertainty estimation, which tend to over-estimate or under-estimate the uncertainty level. Furthermore, these metrics treat the uncertainty estimation of each individual value in a predicted sequence separately, and thus lack an integrated view about the uncertainty of sequential predictions.

To address these challenges, a solution from the CPS community called STL-U [18] developed novel logic-based criteria to measure uncertainty, which is general enough to be applied to any sequential prediction model. It uses these logic-calibrated uncertainty measurements to select and tune the uncertainty estimation schema in deep learning models. At training, the predictive monitoring approach conducts model selection and tuning using STL-U criteria to obtain a well-calibrated uncertainty estimation schema for the RNN-based Bayesian sequential prediction. Intuitively, the satisfaction degree of the predicted sequence (i.e., predicted future states) should be same as the satisfaction degree of the target sequence (i.e., the ground-truth values). STL-U criteria are designed to measure the loss based on the monitoring results and thus evaluates the quality of the uncertainty estimation schema. In this way, the uncertainty estimation schema with the smallest STL-U loss is selected. At runtime, the approach outputs the current and future monitoring results to support ambient intelligence. As a real-time operational scenario, it runs as a continuous iterative process. In this way, the STL-U based predictive monitoring framework provides continuous predictive monitoring of states for decision makers.

The STL-U predictive monitoring approach demonstrates the feasibility of integrating formal methods and Bayesian deep learning for the predictive monitoring of safety and performance requirements in ambient intelligence. In addition, the proposed STL-U criteria can be applied for the uncertainty estimation in a wide range of deep learning applications. Compared with traditional uncertainty estimation methods [9], the proposed logic-based solution can lead to better uncertainty calibration for sequential prediction tasks.

There are open research questions and several directions to explore for future work to address modeling under uncertainty in ambient intelligence. First, the scalability and efficiency of STL-U and other formal monitoring algorithms for more complex specifications (e.g., those with multiple layers of nesting temporal operators) should be further investigated. Secondly, how do humans in the loop affect modeling under uncertainty? Last but not least, how to provide theoretical analysis and guarantees of uncertainty in deep learning models remains an important research question.

V. Robustness and Dependability

The seamless integration of interconnected human-in-the-loop and AI-enabled CPS in ambient intelligence brings about several challenges in ensuring robustness and dependability. How can we ensure robustness to environmental noise, human errors, and accidental or malicious faults targeting the CPS sensors, controllers, and ML components? How can we guarantee robustness given the unpredictable changes in the cyber-physical context, environment, and human behavior? How can we enforce that the ML models satisfy the desired reliability, safety, and security requirements in a given application or set of users? How can we gain the users trust in the robustness and dependability of the system?

With the third wave of AI, future cognitive assistants are envisioned to have human-like reasoning and contextual adaptation capabilities to understand the requirements, recognize new situations, predict future risks, and quickly respond to them. However, existing model-based and data-driven approaches to CPS resilience suffer from: i) reliance on simple physical and behavioral models that cannot fully capture the multidimensional context; ii) using black-box deep learning models that have no knowledge of requirements or cannot be generalized to new situations; iii) passive and delayed detection of anomalies and property violations which prevents timely execution of corrective actions and mitigating risks; and iv) limited consideration of the humans in the loop to gain users trust.

To address the second challenge, STLnet [19] developed a novel formal logic enforced deep learning framework. It guides

the RNN learning process with auxiliary knowledge of model properties, and produces a more robust model for improved future predictions. STLnet is built with a teacher network and a student network. The teacher network is equipped with a STL trace generator, which incorporates the formalized model properties into the learning process. The main idea is that whenever the student network fails to predict a trace (sequence) that follows the model properties, the teacher network generates a trace that is close to the trace returned by the student network and satisfies the model properties simultaneously. The student network then updates its parameters by learning from both the target trace and outcome of the teacher network.

In the training phase, the goal is to teach STLnet to learn from the "correct" traces that follow CPS properties. It first builds a student network, which starts with the basic student network, i.e., a general multivariate RNN. Next, it builds a teacher network, which generates trace that satisfies the model properties expressed in Signal Temporal Logic and has the shortest distance to the original prediction. At last, it trains the network through back propagation with a loss function that is designed with two parts to guide the student network to balance between emulating the teacher's output and predicting the target trace. The network is trained iteratively by repeating these processes until convergence. STLnet is broadly applicable to various sequential prediction tasks beyond smart cities.

This work shows the promise of leveraging formal methods to enhance the robustness and reliability of deep learning. There are many open research problems in this exciting new area that need further studies. For example, how to improve the scalability of formal methods for the property specifications, which involve large-scale sensing data from hundreds of thousands of geographically sparsely distributed locations (sensors)? Can formal logic incorporate all types of properties and constraints from the real world (e.g., physics)? How to develop a generic specification language? How to leverage formal methods to develop reliable deep learning models (e.g., robustness certification) for ambient intelligence?

Recent works on predictive runtime monitoring of safety violations [20] and automated recovery [21] in CPS rely on modeling and inference of human, cyber, and physical context to anticipate impending unsafe systems states and decide on the most effective actions to mitigate safety hazards and prevent incidents. Anomaly detection methods that combine data-driven optimization and ML with the domain knowledge [20], [22], control-theoretic [23]–[25] and physics-based [26] models or behavioral models of human cognition and operation [27], [28] have shown to not only improve the accuracy and timeliness of detection and recovery, but also the transparency and interpretability of models. These attributes are specially important for gaining users trust by providing evidence and explanation on the selected recovery and mitigation actions.

VI. Real-Time and Implementation

For ambient intelligence to be effective it often needs to operate in real-time. It also needs to address realistic deployment problems. Many models (possibly very large) and ML, NLP, and AI algorithms using those models can require costly resources with their answers experiencing long delays. Challenges include reducing the size of models without loss of accuracy and reducing the time delays by more efficient algorithms and by pushing the execution of those algorithms to edge Internet devices or to wearables. These challenges are being addressed along several exciting directions. For example, [29] allows for building a ML solution first without consideration of resource demands. Then a user specifies the resource constraints of the device upon which the solution will execute, e.g., on an edge or wearable device. A compiler then automatically reduces the original model to meet the specifications together with an estimate of loss of accuracy. Continued work along this direction, but considering different models, algorithms, devices, and time requirements could prove valuable. Importantly, the newly developed solutions must also address robustness and uncertainty issues as discussed above. It is also important to not only consider a single solution at a time since the ambient intelligence must synergistically combine many solutions.

The Internet and on-body devices need an infrastructure to support seamless interactions with the exchange of information. The infrastructure needs to permit a very wide variety of devices and associated applications and support evolution of these over time. In ambient intelligence, systems will be exchanging **information** not just data, so determining what and when to exchange information are critical. Many companies provide Internet architectures and associated services. However, we do not believe that these are adequate for the ambient intelligence needs of the future. In particular, the current architectures provide support for data flow from sensors to the cloud and back, but do not focus on how to create and embed ambient intelligence.

VII. Interactivity

With the advance in sensing and actuation, current ambient intelligent systems support a diverse array of interaction including verbal, audio, haptic, or video-based. Although a lot of progress has been made to enable seamless and fluent interaction for intelligent assistants, the complexity of spoken language often makes this challenging due to ambiguity and lack of completeness. Nonverbal interaction is often supported by a haptic interface, visual/ graphical interface, or sensor embedded objects. Recently, a lot of intelligent systems support nonverbal interaction through augmented reality, virtual reality, and mixed reality platforms. Ambient intelligence can consist of multiple modes of interaction among the constituent assistants. For instance, it can provide navigational assistance to visually impaired individuals using multimodal sensing to sense the dynamic environment [30], [31], or assist in robotic surgery [32], [33], or support augmented reality (AR), virtual reality (VR), or mixed reality (MR) enhanced systems [34].

Another aspect of interaction is actuation. Actuation in ambient intelligent systems often involves performing contextual and adaptive interventions. EmIR [35], a social robot for emotional well being of an user tracks user's emotional state through face identification and emotion classification. Upon detecting user's emotion (e.g., happy, angry, sad, disgusted) it mimics user's emotion by changing its physical appearance and sends textual messages to the user to provide contextual reminders and recommendations based on user profile and medical condition. The goal of such actuation or intervention is to persuade the users in activities to lift their emotional state and keep them physically and cognitively active, e.g., reading a book, taking a walk, or spending time with a friend.

Many of these modes of interaction are CPS. Most of these interactions are supported centrally. Recently with the concern of privacy and confidentiality, edge computing seems like a feasible solution. This leads to research opportunities to develop low-resource computational models that can support such interaction in edge devices as well.

Ambient intelligent systems interact with one or more users and the environment. For example, a humanoid, mobile robotic nursing assistant interacts with nurses, patients and tele-operators [36]. It lifts and transports a patient from one location to another inside a hospital based on the command from a nurse and interacts with a tele-operator through a visual interface where the operator can see and control its movements to ensure safety. For seamless interaction, the challenges are that ambient intelligent systems should support data flow between users and environment, protect user privacy, user identification and tracking, and perform online learning of user profile. It should support the communication among constituent cognitive assistants, e.g., a cognitive assistant to support elderly in performing daily activities should be able to interact with the personal assistant of the corresponding user (e.g., Alexa or Google Home) for weather updates and schedule the user's daily routine accordingly. They should support identifying new users, learning new events, and detecting relevant change in user and environment. For instance intelligent systems are often trained on user's voice, gait, or facial features to identify and track user. A user might experience change in their voice due to a disease or condition (e.g., throat cancer, alcohol abuse, thyroid disorders). The speaker identification module of a cognitive or ambient assistant should be sensitive to such change. Ambient intelligence design should have provision to accommodate such changes to ensure effective interaction.

Recent advances in ambient and cognitive assistants result in technical innovation to enable natural and often proactive interaction. Natural language generation has been a popular choice to support domain specific natural verbal interaction for cognitive and ambient intelligent assistants. For natural interaction, ambient intelligence should be aware of user context. For example, providing hands-free interface for interaction when user's hands are occupied [37] by tracking user's hand movement through depth camera or wearable sensors, providing haptic feedback instead of auditory to not interrupt user when they are busy or engaged (e.g., vibration in steering wheel when user is driving).

Most cognitive and ambient intelligent systems are reactive. Occasionally, such intelligent systems are designed to be proactive for a set of predefined contexts. Such as, detecting unsafe movement for users who are undergoing physical therapy and post-injury rehabilitation [38], proactive monitoring of surgical device malfunctions to avoid preventable surgical errors [39], or alerting an individual if they forget their keys or phone while leaving the home [40]. While proactive monitoring can be effective for many ambient intelligence applications, some safety-critical applications demand considering the trade-off between false positives (FP) and false negatives (FN) for delivering intervention. For example, for user activity monitor, FPs are not costly. But for ambient intelligence in the ICU or emergency FPs are costly [41], [42]. In such cases being selectively proactive or even being more reactive might be more effective, e.g., only give feedback when asked and when the system is confident enough [11], [28].

Research in seamless coordination and integration of multiple intelligent assistants in an ambient intelligent environment is still minimally explored [1]. New research will benefit from automatic techniques for metadata collection and common data dictionary, time synchronization of different dependent modules of assistants, and context-aware actuation of individual intelligent components.

VIII. Conflicts

Ambient intelligence requires seamless and synergistic interactions between cognitive assistants found on the body and in-situ. Due to the dynamics of environments, individual personal behaviors, individuals' objectives, and competing resource needs, conflicts will arise. Therefore, it is necessary for ambient intelligence to support detecting and resolving conflicts. It is also possible that knowledge bases and current context obtained from sensors which are held by a particular cognitive assistant have ambiguous or even contradictory data. These situations must also be detected and resolved in an intelligent manner. Consequently, dynamically detecting and resolving conflicts are major challenges for ambient intelligence. Possible solution directions include building upon CPS research that has addressed these issues in smart homes, smart health, and smart cities. See Figure 3

For smart homes, DepSys [43] was a system that provided comprehensive strategies to specify, detect, and resolve conflicts by addressing a spectrum of dependencies including requirements, name, and control dependencies. DepSys also handles the case when app developers fail to specify dependencies. DepSys automatically resolves conflicts in controlling sensors and offers a strategy for resolving control conflicts of actuators. DepSys also detects conflict across smart devices by considering their impact on the environment, e.g., one app is running a humidifier and another app is running a dehumidifier at the same time. In DepSys solutions are based on rules. While some of these strategies can be applied to cognitive assistance and ambient intelligence there are still open issues

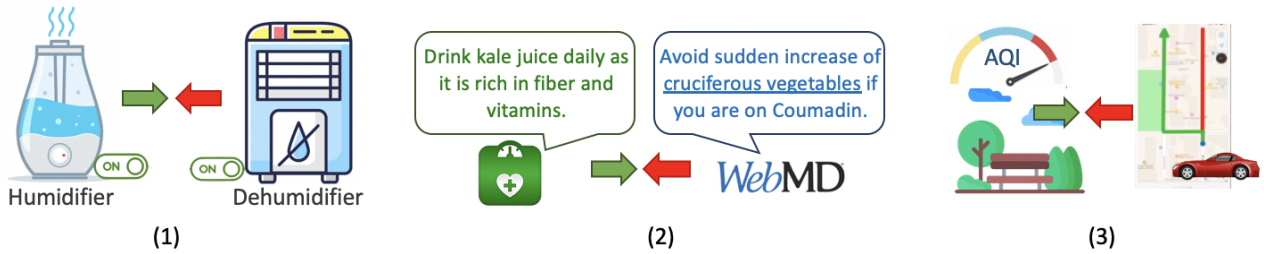

Fig. 3. Conflicts in Ambient Intelligence: (1) In a smart home, one app is running a humidifier and another app is running a dehumidifier at the same time. (2) People get conflicted health advice from different health care apps. (3) In a smart city, increase of pollution in near a park is caused by a primary decision of redirecting traffic to that area.

with respect to how would rule based systems evolve over time and how would they incorporate other complexities found in ambient intelligence across much broader context than smart homes.

In smart health, the EyePhy system [44] detected dependencies across interventions of human-in-the-loop CPS medical apps. It used a physiological simulator called HumMod [45] that can model the complex interactions of the human physiology using over 7800 variables capturing cardiovascular, respiratory, renal, neural, endocrine, skeletal muscle, and metabolic physiology. It uses a physiological simulator to detect dependencies has many advantages. First, it allows performing dependency analysis across a wide range of physiological parameters. Second, it enables accounting for drug dosage and the time gap between the interventions in the dependency analysis. Third, the dependency analysis is personalized, e.g., if someone has heart related problems, the dependency analysis can be focused on the heart. An important question is how does a cognitive assistant model and predict future situations to determine if there might be a conflict in the future. In EyePhy, a simulator was used. Simulators and other techniques, e.g., those based on ML modeling and prediction must be developed.

Cognitive assistants will help improve healthcare. However, conflicting health information is one of the primary barriers of self-management of chronic diseases and wellbeing. This problem is growing with the prevalence of pervasive digital health care applications. Increasing number of people now rely on mobile health apps and online health websites to meet their information needs and often receive conflicting health advice from these sources. This problem is more prevalent and severe in the setting of multi-morbidities. In addition, often medical information can be conflicting with regular activity patterns of an individual. Therefore, for cognitive assistance to be effective in healthcare they must solve the problem of finding conflicts in heterogeneous health applications including health websites, health apps, online drug usage guidelines, daily activity logging applications, and cognitive assistants.

Preclude2 [46] developed a comprehensive taxonomy of conflicts based on the semantics of textual health advice and activities of daily living. But, finding conflicts in health applications poses its own unique lexical and semantic challenges. These include large structural variation between text and hypothesis pairs of advice, finding conceptual overlap between pairs of advice, inference of the semantics of an advice (i.e., what to do, why and how) and activities, and aligning activities suggested in advice with the activities of daily living based on their underlying dependencies and polarity. In Preclude2, a novel semantic rule-based solution to detect conflicts in activities and health advice derived from heterogeneous sources was developed. In addition, Preclude2 considers personalization and context- awareness while detecting conflicts.

Now consider conflicts in smart cities. A smart city is a system of systems, where each system represents a specific domain (e.g., transportation, public safety, utility, emergency, environment, city planning and operations) and each domain consists of a set of services. For example, the public safety domain may include police patrolling services, traffic violation control services, and road accident management services. Each service performs a set of functions to fulfill objectives, e.g., a traffic violation control service penalizes drivers for speeding. Functions may produce a set of effects upon completion, e.g., blocking a lane for road work. Effects that are directly actuated by a service are primary effects. Effects that are the outcomes of a primary effect are characterized as secondary effects such as increase of pollution in an area due to a primary decision of redirecting traffic to that area. Thus, a single action can create a chain of subsequent effects. Developing ambient intelligence in smart cities is very challenging including those challenges related to detecting and resolving conflicts.

The CPS field has addressed conflict detection and resolution in smart cities in various ways. One approach uses formal methods to specify requirements, i.e., by using Signal Temporal Logic (STL). But STL is not sufficient to represent all the complexities of smart cities. Extensions to STL, e.g., SaSTLs [47] has extended STL to handle spatial and aggregation type requirements. Consequently, SaSTL can be used to specify Point of Interests (PoIs), physical distances, spatial relations of the PoIs and sensors, aggregation of signals over locations, degree/percentage of satisfaction, and temporal requirements. There are on-going challenges in expanding solutions in this area to more and more complex situations found in ambient intelligence.

Once conflicts are detected they must be resolved. This is

extremely complicated due to many things including uncertainty in the environment, competing objectives, and resource limitations. In CPS, one solution CityResolver [48] uses an Integer Linear Programming based method to generate a small set of resolution options. An open question is whether this approach can be successful in the broader context of ambient intelligence.

IX. Comprehensive Context

Almost all significant applications of AI and CPS require context to perform adequately. Consequently, this is a well-researched field. The in-situ sensors used as infrastructure for ambient intelligence together with wearables can provide the basis for comprehensive context. This could include personalized context as determined by sensing physiological, psychological, behavioral, time, space, environmental, and other parameters. However, to improve ambient intelligence many challenges exist, including the following. One, what context should be used at a given instance of time to provide an intelligent response? Two, how to adjust the need and type of context over time. Three, what context should be forgotten. Four, what context should be remembered and how. Five, how to detect the difference between an anomaly and new patterns. Six, how to detect and address context that arises between individuals or groups of people. Seven, how to detect behaviors in complex scenes. Eight, how to intelligently use context that may be shared yet maintain privacy.

CPS technologies of sensing, sensing with confidence, multi-modal sensing, sensor fusion, actuations, and signal processing, in general, can be applied to support the use of comprehensive context. New CPS technologies such as smart textiles and smart skin can increase the availability of contextual data. However, we believe that the challenges listed above have not yet been adequately addressed. We suggest that new research in the integration of AI and CPS is needed to solve these problems. For example, smart skin may be able to detect high anxiety of a person, but the AI decision making still does not recommend medication at this time due to other physiological states, and physical context of where the person is or what they are doing that perhaps indicates there should be no medication that may make the person drowsy.

X. Dynamic Adaptation and Learning

For cognitive assistants to become the backbone of ambient intelligence they must meet the challenges to dynamically adapt to current situations and learn over time. Adaptation refers to having the cognitive assistant change its behavior in response to its environment, but in this context the environment has a very broad meaning. This includes adapting to users' goals, actions, and behaviors, other peoples general behaviors, the users' health, mental and physical, and the state of the surrounding world, including environmental states, predicted future states, failures and faults, and the ambient intelligence infrastructure itself.

Given such a complicated problem there will be ambiguity, conflict (see Section VIII), and uncertainty (see Section IV), all of which are key challenges that must be addressed by the adaptive decision making component of the cognitive assistant. The adaptive decision making will result in various outcomes. Learning what worked and what did not work and incorporating that into the knowledge base of the cognitive assistant is an essential requirement for the ability of the cognitive assistant to maintain good performance over time.

Principles from CPS are needed to accurately sense the environment in the broad sense as described above, and adapt. CPS sensing technology can provide a comprehensive collection of sensors and sensor fusion algorithms to improve situation awareness, a critical component for ambient intelligence. Adaptive and robust control theory can potentially be applied to better place adaptation on a carefully analyzed foundation. Reinforcement learning and control theory already exhibit shared principles. CPS have been applying model-based design to improve reinforcement learning [49] and applying verification techniques to safe exploration in reinforcement learning [50], [51].

Since learning is the process of synthesizing new knowledge and connecting new information and experiences with existing knowledge, having robust and modifiable models is important. Hence, techniques described in Section V for developing robust models under uncertainty are applicable for adaptation and control as well.

CPS have also applied control theory in a manner that accounts for realistic implementation issues in tools such as TrueTime and Jitterbug [52]. These types of results can possibly support not only the theory and analysis of adaptation and learning, but also its realistic implementation.

XI. Security

Security is a general issue that must be addressed in almost all systems. However, with the advance of smart devices and the Internet of Things (IoT), new security issues are created [53]–[55]. In [55], the authors provide a CPS security attack taxonomy defined based on new problems for the (i) cyber, (ii) the physical, and (iii) the cyber physical aspects of a system. For example, cyber attacks include denial of service and malware. Physical attacks include supply chain attacks, signal jamming, sensor spoofing, transduction and tampering as examples. Cyber physical attacks include identity and device spoofing, denial of service, relay attacks, and control system instability. While these attacks can occur in all systems on the Internet, they take on potential safety critical consequences when perpetrated in smart devices and cognitive assistants that are, at least partially, relying on physical devices. Consequences could include heart and insulin pumps being manipulated and causing serious medical problems including death, and cognitive assistants providing wrong information and advice, also potentially causing serious health outcomes.

Current CPS research is primarily focusing on all forms of physical attacks, on control loop attacks, and attacks on ML models used in CPS systems. Physical attacks often change the sensor readings in various ways. Research directions

try to exploit redundant or related sensing modalities (e.g., temperature, pressure and volume sensors related to each other by physics) to detect and resolve attacks [56]. Other physical attacks include jamming of wireless communications. Frequency hopping, spread spectrum and other techniques can provide some resilience to jamming. Transduction attacks [53] exploit the use of sensors in ways they were not originally intended. See [53] for examples. A related attack called the Dolphin attack [57] uses inaudible sounds to falsely send commands to a device such as Alexa or Siri which can be considered a basis for cognitive assistance. In general, physical layer solutions must include better frequency filters and signal processing to avoid having the resonances from ultrasound to appear in the voice frequency range. Solutions are also needed in the manufacture of circuits to reduce the effects of resonance, increase the frequency of checking sensor output by software, and even careful layout of components on system boards to minimize unwanted coupling.

Feedback control loops are critical components of many CPS, including industrial control systems, supervisory control and data acquisition systems, autonomous vehicles, and medical devices. In a control loop attack, the adversary usually seeks to cause instability, thereby causing the system to malfunction. Often, to detect these attacks requires a deep understanding of the physics of the process being controlled as well as the logic that controls the equipment. Standard security solutions can reduce the threat surface, but they often do not provide the necessary coverage in a complex system with a variety of sensors and actuators. A promising approach is fuzzing [58]. In fuzzing, inputs are automatically generated where the goal is to force coverage of unexplored code. The technique is particularly applicable to CPS where the range of possible inputs is difficult to enumerate or bound.

ML attacks occur when an attacker develops adversarial examples, i.e., inputs with small perturbations (sometimes imperceptible) that cause a trained ML model to misclassify. Solutions include work to increase the robustness of the data driven models being used. See the above section on robustness and dependability for solution directions that also apply to security. Adversarial ML attacks are a relatively new threat to CPS and there is still much research to understand the nature of the attacks and how to build robust ML models that are not susceptible to adversarial manipulation of the physical artifacts (e.g., signs, images, audio, etc.) that are inputs to the system. Cognitive assistants often rely on verbal exchanges which can be attacked [59] so more secure audio capture and transcription are required. ML, while it can be attacked, can also support security. For example, deep learning algorithms can use speech to identify people and subsequently could be applied to ensure that the cognitive assistant is dealing with the correct person.

XII. Summary

While ambient intelligence is an AI problem, it is also a CPS problem because much of the information to be used by ambient intelligence will come from smart devices and the IOT. This paper identifies key challenges and opportunities for the integration of AI and CPS. It also describes how various CPS technologies (with extensions) can potentially support guarantees and safety for ambient intelligent systems. Of course, as we point out throughout the paper, many challenges remain.

In this paper we are not comprehensive, rather we chose representative and important research challenges to address. Other key challenges and areas are not addressed, including, privacy, fairness, biases, reasoning, interpretability, immersive robotics, etc.

References

[1] S. M. Preum, S. Munir, M. Ma, M. S. Yasar, D. J. Stone, R. Williams, H. Alemzadeh, and J. A. Stankovic, "A review of cognitive assistants for healthcare: Trends, prospects, and future directions," *ACM Computing Surveys (CSUR)*, vol. 53, no. 6, pp. 1–37, 2021.

[2] C. Ramos, J. C. Augusto, and D. Shapiro, "Ambient intelligence—the next step for artificial intelligence," *IEEE Intelligent Systems*, vol. 23, no. 2, pp. 15–18, 2008.

[3] F. Sadri, "Ambient intelligence: A survey," *ACM Computing Surveys (CSUR)*, vol. 43, no. 4, pp. 1–66, 2011.

[4] A. Haque, A. Milstein, and L. Fei-Fei, "Illuminating the dark spaces of healthcare with ambient intelligence," *Nature*, vol. 585, no. 7824, pp. 193–202, 2020.

[5] M. LLC. (2016) Intelligent cognitive assistants: Workshop summary and recommendations. [Online]. Available: https://www.nsf.gov/crssprgm/nano/reports/2016-1003_ICA_Workshop_Final_Report_2016.pdf

[6] D. C. Engelbart, "Augmenting human intellect: A conceptual framework," *Menlo Park, CA*, 1962.

[7] D. Isern and A. Moreno, "A systematic literature review of agents applied in healthcare," *Journal of medical systems*, vol. 40, no. 2, p. 43, 2016.

[8] A. K. Noor, "Potential of cognitive computing and cognitive systems," *Open Engineering*, vol. 5, no. 1, pp. 75–88, 2015.

[9] Z. Chen and B. Liu, "Lifelong machine learning," *Synthesis Lectures on Artificial Intelligence and Machine Learning*, vol. 12, no. 3, pp. 1–207, 2018.

[10] N. E. ElHady and J. Provost, "A systematic survey on sensor failure detection and fault-tolerance in ambient assisted living," *Sensors*, vol. 18, no. 7, p. 1991, 2018.

[11] S. Preum, S. Shu, M. Hotaki, R. Williams, J. Stankovic, and H. Alemzadeh, "Cognitiveems: A cognitive assistant system for emergency medical services," *ACM SIGBED Review*, vol. 16, no. 2, pp. 51–60, 2019.

[12] M. A. Rahman, S. M. Preum, R. Williams, H. Alemzadeh, and J. A. Stankovic, "Grace: Generating summary reports automatically for cognitive assistance in emergency response," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, no. 08, 2020.

[13] Y. Gal and Z. Ghahramani, "Dropout as a bayesian approximation: Representing model uncertainty in deep learning," in *Proc. of ICML 2016*, vol. 48. JMLR.org, 2016, pp. 1050–1059. [Online]. Available: http://proceedings.mlr.press/v48/

[14] L. Zhu and N. Laptev, "Deep and confident prediction for time series at Uber," in *Proc. of ICDM Workshops*. IEEE, 2017, pp. 103–110.

[15] D. J. MacKay, "A practical bayesian framework for backpropagation networks," *Neural computation*, vol. 4, no. 3, pp. 448–472, 1992.

[16] Y. Xiao and W. Y. Wang, "Quantifying uncertainties in natural language processing tasks," in *Proc. of the AAAI 2019*, vol. 33, 2019, pp. 7322–7329.

[17] A. Kendall and Y. Gal, "What uncertainties do we need in bayesian deep learning for computer vision?" in *Proc. of NIPS 2017*, 2017, pp. 5574–5584.

[18] M. Ma, J. Stankovic, E. Bartocci, and L. Feng, "Predictive monitoring with logic-calibrated uncertainty for cyber-physical systems," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 20, no. 5s, pp. 1–25, 2021.

[19] M. Ma, J. Gao, L. Feng, and J. A. Stankovic, "Stlnet: Signal temporal logic enforced multivariate recurrent neural networks." in *NeurIPS 2020*, 2020.

[20] X. Zhou, B. Ahmed, J. H. Aylor, P. Asare, and H. Alemzadeh, "Data-driven design of context-aware monitors for hazard prediction in artificial pancreas systems," in *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2021, pp. 484–496.

[21] L. Zhang, X. Chen, F. Kong, and A. A. Cardenas, "Real-time attack-recovery for cyber-physical systems using linear approximations," in *2020 IEEE Real-Time Systems Symposium (RTSS)*, 2020, pp. 205–217.

[22] K. R. Varshney and H. Alemzadeh, "On the safety of machine learning: Cyber-physical systems, decision sciences, and data products," *Big data*, vol. 5, no. 3, pp. 246–255, 2017.

[23] H. Choi, W.-C. Lee, Y. Aafer, F. Fei, Z. Tu, X. Zhang, D. Xu, and X. Deng, "Detecting attacks against robotic vehicles: A control invariant approach," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 801–816.

[24] A. Ding, P. Murthy, L. Garcia, P. Sun, M. Chan, and S. Zonouz, "Mini-me, you complete me! data-driven drone security via dnn-based approximate computing," in *24th International Symposium on Research in Attacks, Intrusions and Defenses*, 2021, pp. 428–441.

[25] D. Pritam, L. Guanpeng, C. Zitao, K. Mehdi, and P. Karthik, "Pid-piper: Recovering robotic vehicles from physical attacks," in *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2021.

[26] R. Quinonez, J. Giraldo, L. Salazar, E. Bauman, A. Cardenas, and Z. Lin, "SAVIOR: Securing autonomous vehicles with robust physical invariants," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 895–912.

[27] M. Yasar and H. Alemzadeh, "Real-time context-aware detection of unsafe events in robot-assisted surgery," in *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2020, pp. 385–397.

[28] S. Shu, S. Preum, H. M. Pitchford, R. D. Williams, J. Stankovic, and H. Alemzadeh, "A behavior tree cognitive assistant system for emergency medical services," in *2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2019, pp. 6188–6195.

[29] S. Bhattacharya and N. D. Lane, "Sparsification and separation of deep learning layers for constrained resource inference on wearables," in *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, 2016, pp. 176–189.

[30] H. Vorobieva, M. Soury, P. Hède, C. Leroux, and P. Morignot, "Object recognition and ontology for manipulation with an assistant robot," in *International Conference on Smart Homes and Health Telematics*. Springer, 2010, pp. 178–185.

[31] M. E. Pollack, L. Brown, D. Colbry, C. Orosz, B. Peintner, S. Ramakrishnan, S. Engberg, J. T. Matthews, J. Dunbar-Jacob, C. E. McCarthy *et al.*, "Pearl: A mobile robotic assistant for the elderly," in *AAAI workshop on automation as eldercare*, vol. 2002, 2002, pp. 85–91.

[32] A. Shademan, R. S. Decker, J. D. Opfermann, S. Leonard, A. Krieger, and P. C. Kim, "Supervised autonomous robotic soft tissue surgery," *Science translational medicine*, vol. 8, no. 337, 2016.

[33] O. Weede, A. Bihlmaier, J. Hutzl, B. P. Müller-Stich, and H. Wörn, "Towards cognitive medical robotics in minimal invasive surgery," in *Proceedings of Conference on Advances In Robotics*. ACM, 2013.

[34] F. Ribeiro, D. Florencio, P. A. Chou, and Z. Zhang, "Auditory augmented reality: Object sonification for the visually impaired," in *2012 IEEE 14th international workshop on multimedia signal processing (MMSP)*. IEEE, 2012, pp. 319–324.

[35] J. A. Rincon, A. Costa, P. Novais, V. Julian, and C. Carrascosa, "A new emotional robot assistant that facilitates human interaction and persuasion," *Knowledge and Information Systems*, pp. 1–21, 2018.

[36] J. Hu, A. Edsinger, Y.-J. Lim, N. Donaldson, M. Solano, A. Solochek, and R. Marchessault, "An advanced medical robotic system augmenting healthcare capabilities-robotic nursing assistant," in *2011 IEEE international conference on robotics and automation*. IEEE, 2011, pp. 6264–6269.

[37] A. Neumann, C. Elbrechter, N. Pfeiffer-Leßmann, R. Kõiva, B. Carlmeyer, S. Rüther, M. Schade, A. Ückermann, S. Wachsmuth, and H. J. Ritter, "Kognichef: A cognitive cooking assistant," *KI-Künstliche Intelligenz*, vol. 31, no. 3, pp. 273–281, 2017.

[38] V. Rajanna, P. Vo, J. Barth, M. Mjelde, T. Grey, C. Oduola, and T. Hammond, "Kinohaptics: An automated, wearable, haptic assisted, physio-therapeutic system for post-surgery rehabilitation and self-care," *Journal of medical systems*, vol. 40, no. 3, p. 60, 2016.

[39] E. Rajih, C. Tholomier, B. Cormier, V. Samouëlian, T. Warkus, M. Liberman, H. Widmer, J.-B. Lattouf, A. M. Alenizi, M. Meskawi *et al.*, "Error reporting from the da vinci surgical system in robotic surgery: A canadian multispecialty experience at a single academic centre," *Canadian Urological Association Journal*, vol. 11, no. 5, p. E197, 2017.

[40] D. Sonntag, "Kognit: Intelligent cognitive enhancement technology by cognitive models and mixed reality for dementia patients," in *2015 AAAI Fall Symposium Series*, 2015.

[41] S. Ansari, A. Belle, H. Ghanbari, M. Salamango, and K. Najarian, "Suppression of false arrhythmia alarms in the icu: a machine learning approach," *Physiological measurement*, vol. 37, no. 8, p. 1186, 2016.

[42] S. M. Preum, S. Shu, J. Ting, V. Lin, R. Williams, J. Stankovic, and H. Alemzadeh, "Towards a cognitive assistant system for emergency response," in *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2018, pp. 347–348.

[43] S. Munir and J. A. Stankovic, "Depsys: Dependency aware integration of cyber-physical systems for smart homes," in *2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2014, pp. 127–138.

[44] S. Munir, M. Ahmed, and J. Stankovic, "Eyephy: Detecting dependencies in cyber-physical system apps due to human-in-the-loop," in *proceedings of the 12th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services on 12th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2015, pp. 170–179.

[45] R. Hester, A. Brown, L. Husband, R. Iliescu, W. A. Pruett, R. L. Summers, and T. Coleman, "Hummod: a modeling environment for the simulation of integrative human physiology," *Frontiers in physiology*, vol. 2, p. 12, 2011.

[46] S. M. Preum, A. S. Mondol, M. Ma, H. Wang, and J. A. Stankovic, "Preclude2: Personalized conflict detection in heterogeneous health applications," *Pervasive and Mobile Computing*, vol. 42, 2017.

[47] M. Ma, E. Bartocci, E. Lifland, J. Stankovic, and L. Feng, "Sastl: spatial aggregation signal temporal logic for runtime monitoring in smart cities," in *2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2020, pp. 51–62.

[48] M. Ma, J. A. Stankovic, and L. Feng, "Cityresolver: a decision support system for conflict resolution in smart cities," in *Proc. of ICCPS 2018*. IEEE Computer Society / ACM, 2018, pp. 55–64.

[49] M. H. Cohen and C. Belta, "Model-based reinforcement learning for approximate optimal control with temporal logic specifications," in *Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control*, 2021, pp. 1–11.

[50] N. Hunt, N. Fulton, S. Magliacane, T. N. Hoang, S. Das, and A. Solar-Lezama, "Verifiably safe exploration for end-to-end reinforcement learning," in *Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control*, 2021, pp. 1–11.

[51] M. Abate, M. Mote, E. Feron, and S. Coogan, "Verification and runtime assurance for dynamical systems with uncertainty," in *Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control*, 2021, pp. 1–10.

[52] C. Anton, H. Dan, L. Bo, E. Johan, and E. Karl, "How does control timing affect performance," *IEEE Contr. Syst. Mag*, vol. 23, pp. 16–30, 2003.

[53] K. Fu and W. Xu, "Risks of trusting the physics of sensors," *Communications of the ACM*, vol. 61, no. 2, pp. 20–23, 2018.

[54] M. Krotofil, "Evil bubbles or how to deliver attack payload via the physics of the process," *Blackhat Briefings*, 2017.

[55] J. A. Stankovic and J. Davidson, "Raising awareness of security challenges for the internet of trillions of things," *NAE Bridge Magazine*, vol. 49, no. 3, pp. 40–45, 2019.

[56] J. A. Stankovic, T. Le, A. Hendawi, and Y. Tian, "Hardware/software security patches for the internet of things," in *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*. IEEE, 2021, pp. 240–245.

[57] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 103–117.

[58] B. P. Miller, L. Fredriksen, and B. So, "An empirical study of the reliability of unix utilities," *Communications of the ACM*, vol. 33, no. 12, pp. 32–44, 1990.

[59] N. Carlini and D. Wagner, "Audio adversarial examples: Targeted attacks on speech-to-text," in *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018, pp. 1–7.