AN EVENT DRIVEN FRAMEWORK FOR ASSISTIVE CPS ENVIRONMENTS

Fillia Makedon[1], Zhengyi Le[1], Heng Huang[1], Eric Becker[1], Dimitrios Kosmopoulos[2]
{makedon, zyle, heng, becker}@uta.edu, dkosmo@iit.demokritos.gr
[1]Computer Science and Engineering Department, University of Texas at Arlington, USA
[2]The Institute of Informatics and Telecommunications, the NCSR Demokritos, Greece

Abstract

***Assistive Cyberphysical Systems** (ACPS) are pervasive and ubiquitous systems connecting the cyber with the physical worlds, with the aim to assist a human's daily activities both at home and at work. We present an **event driven framework** with event identification mechanisms that drive actuators, transform a substrate and alter human behavior in a feedback loop process that allows a human to control her ACPS. This framework is a dynamic, context aware, adaptive, self-repairing and high-confidence system that couples computational power with physical substrate (testbed) control and command; it monitors human activities with differential privacy and security capabilities, recognizes events, human needs from lifestyle, and processes environmental and longitudinal health data.*

1. INTRODUCTION

Assistive Cyber-Physical Systems or ACPS are cyberphysical systems that collect data and provide assistance to humans interacting with the physical and digital environment around them. In this special CPS category, the human is dependent on the input and output of instruments and on the environment's sensors embedded in @home and @work spaces. ACPS is a complex, dynamic and pervasive CPS that is human-centered and responsive to human needs.

In this paper, we describe an "***event identification mechanism***" for ACPS that enables seemingly meaningless human activity and interaction data to gain meaning with regard to human behavior. This mechanism has self-learning capabilities and becomes more accurate with time and usage. **Event identification (EI),** is a 2-phase process of first assimilating continuous and discrete types of data or streams collected through various types of sensors over time and then identifying "events" of interest through the use of various mining and feature extraction tools applied to multi-channel data in a multi-layered non-invasive and privacy-preserving approach. Through the EI mechanism, the framework can summarize and filter non-interoperable information over time and space in order to reach higher levels of awareness and intelligence that responds to patterns and enhances human capabilities in significant ways.

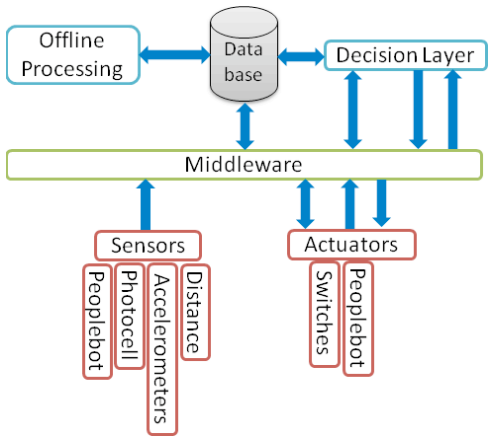

Figure 1 ACPS Framework for Event Detection

ACPS desired properties include (1) a self-correcting and adjusting feedback loop that refines the identification of an event by adjusting sensors and data collected; (2) flexible and easy to use human-centered and customizable functions; (3) an expandable architecture to accommodate new types of instruments and devices; (4) responsiveness to emergency and non-emergency situations; (5) supportive prediction and decision making by identified events; (6) an EI mechanism that can allow human intervention and control in ways that adapt to different situations, the types of data that need to be collected, new technologies or software. This mechanism can be used to discover behavioral and environmental "markers" of social and community importance that can trigger alerts or warnings or address social and community needs, ranging from better learning or training environments, to improving human performance in stressed situations, such as recognizing depression, pain, lack of

understanding, or even recklessness in the face of risk or danger; (7) ability to support the design and innovation of new instruments, as well as test and evaluate new ways to use them; (8) powerful backend analysis engines to recognize low-level and higher level events, in ways that support meta-analysis impacting numerous CPS applications, from healthcare, to manufacturing, house/car design, training, school scheduling [2,5-10]. Figure 1 shows the ACPS framework for event detection.

2. EVENT DRIVEN ACPS

An ACPS "Event" is defined as any extraordinary occurrence or observation involving the subjects, objects, and environmental status in the entire environment. We focus on identifying three types of events [3,4]: (a) prevention of accidents such as falls or other injuries; (b) abnormal behavior or activity involving either the human or the system, (e.g., malfunctioning of instruments, physical or digital intrusions, aberration from normal human activity (e.g. missed medication intake or meals) in order to better guide the human or signal the need for the system and/or its components to self-correct or ask for human intervention; (c) acute social/psychological need detected (e.g., depression, pain, loneliness). All events in ACPS can be organized as a hierarchical tree: the top-level events are derived from the low-level events. The event identification component in the ACPS framework gets data fed from multimodal sensors and devices. In ACPS, event identification and fusion exist both at low-level data processing (e.g. identify abnormal activities from image/video) and high-level data processing (e.g. identify events from correlated events and data from different sensors/devices).

3. FEEDBACK LOOP

This ACPS includes a self-correcting and adjusting *feedback loop* that refines the identification of an event by adjusting the way the sensors and the environment collect data. For example, reduce noise by adding more sensors, adjust the window of time over which data are collected to, e.g., prevent data leakage; improve the algorithm applied on data fusion, etc. Figure 2 shows the feedback loop of the ACPS framework for event detection. The following takes place. (a) The data collection module collects raw sensory data from the static sensors; the data are then processed by the *behavior recognition components* to create events. (b) The events are fed into the *Event Processing/Identification Module*. (c) Unusual behaviors (predefined by customized parameters) are identified and sent to the *human operator* (who may or may not intervene to close the loop) and/or to the *actuator controller* who may trigger a certain set of actions. (d) The actuator controller activates the robot or moving cameras to focus their sensors on the target. (e) The system may direct for better sensory input to be acquired and sent to the *behavior recognition module*. (f) Some live video can be optionally transmitted to the human operator, who closes the loop. In summary, there is the option for a human operator to control the loop or have it operate in automatic mode.

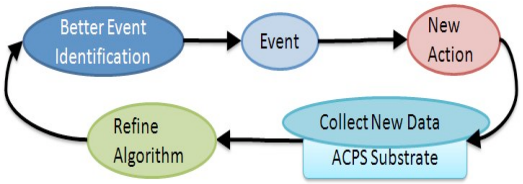

Figure 2 Event Refinement Feedback Loop

4. DATA MODEL AND DIMENSION REDUCTION FOR ACPS DATA

An ACPS system has to deal with massive and highly heterogeneous types of data, which require advanced processing algorithms and methods to be feasible. The ACPS Data stream values are often associated with multiple aspects. For example, each value from environmental sensors may have an associated type (e.g., temperature, sound, EMG signal, etc) as well as location. The index of the data array is usually larger than 3 (also considering the time stamp). Traditional data modeling methods such as, PCA/SVD do not

work for such multi-array (tensor) datasets, neither do vectors, or exact 3D or higher order tensors. Instead, we use *tensor decomposition methods* [26-28] to model such streams, remove outliers, and simultaneously find patterns within and across the multiple aspects. The *tensor decomposition method* we use can be summarized as follows: given an input tensor $X \in R^{n_1 \times n_2 \times \ldots \times n_M}$ and core tensor sizes $\{r_1, r_2, \ldots r_M\}$, find a core tensor $y \in R^{r_1 \times r_2 \times \ldots \times r_M}$ and a sequence of projection matrices $U^{(d)} \mid_{d=1}^{M} \in R^{n_d \times r_d}$ such that $\| X - y \times_1 U^{(1)} \cdots \times_M U^{(M)} \|$ is minimized, i.e., $X \approx y \times_1 U^{(1)} \cdots \times_M U^{(M)}$. For example, a 3rd order tensor $X \in R^{I_1 \times I_2 \times I_3}$ can be decomposed to $X \approx y \times_1 U \times_2 V \times_3 W$ where $y \in R^{R_1 \times R_2 \times R_3}$ is the core tensor, *U*, *V*, and *W* are the projection matrices, the indices I_1, I_2, I_3 are three different aspects, e.g. temperature, location, time. Using the tensor decomposition method, we can compress the original tensor to get an approximation tensor with much less data size. The main components of original data are still kept. The redundant information and outliers are also removed. Thus, the low approximation of tensor data will help the pattern mining and event identification.

The heterogeneous data could be easily modeled as a high-order tensor data and analyzed by the above method. For example, the data from temperature and light sensors can be modeled as a 4-diemsnional tensor: *time* × *location* × *temperature* × *light values.* Tensor decomposition method can efficiently help us reduce the redundancy and find patterns from heterogeneous data.

5. PRIVACY AND SECURITY ISSUES

The ACPS system produces, by its nature, valuable behavioral and other human-centered data that relate to sensitive health records of a person. It can also connect to biomedical data such as brain (e.g., fMRI/MRI) scans, history of a condition, physical characteristics and even genetic characteristics that impact the definition of an event (e.g., if the person has Multiple Sclerosis which exhibits recurring motor behavior depending on the medication). Given the interrelationships of sensitive data involved in an ACPS environment, if we are to produce robust and feasible ACPS systems for broad remote e-health use in pervasive environments of the future, we address all issues of privacy and security as an integral part of data modeling and processing. In particular, we want to ask questions such as, at which points of the event identification process is there risk for privacy violations or security lapses? Or, how does each stage of the Event Identification process rank in terms of data sensitivity? In this section, we provide an analysis of the different types of security issues that can arise.

In a series of PETRA'08 and 09, papers [1, 11-13], we have introduced a security framework for ACPS where we divide the key privacy and security issues in two different types: *Low level security* that applies to raw data or streams and *high level security* issues that take place during high level events where we have more semantic meaning associated with each event, regarding human behavior. Regarding the low-level security issues, we consider *Data Integrity*, i.e., that nobody tampered with the data and no parts are missing, *Confidentiality*, where data is encrypted and only the proper receiver can decrypt it, and *Availability*, that ensures continued and robust service (details are in Section 5.1). Regarding the high-level security issues, we consider sensitive events that are defined by the user or the data owner. The details are presented in the following subsection 5.2.

5.1 Low Level Security on Raw Data Sets/Streams

Data Integrity: When data are generated in devices and ready to be sent to a receiver, (such as a base station, a router or another device which will further process the data), we are supposed to guarantee that ACPS can tell that (1) it receives the entire package of the data instead of a portion of it, and that (2) the data is from that device and not from somewhere or someone else [2,3]. This can

usually be provided by generating the hash value or fingerprint of the entire message or data sequence, and then by signing the hash value with the private key of the device, if public key operations are affordable on that device. If public key operations are not affordable on a given device, data integrity can be assured by using a keyed hash function to generate the fingerprint and the two parties having established a shared symmetric key. The receiver will use the public key of the sender or the symmetric key they shared prior to verify the package it received. The fingerprint makes sure that all the original information was included and the keyed hash or the digital signature makes sure that the data is generated by the device which holds the same key or corresponding public key.

Data Confidentially: When data is transmitted among devices, secure channels must be established for the communication to protect the data against eavesdroppers, which can be a major problem in a wireless environment. Therefore, besides the data origination authentication and integration checking, the data must be encrypted during transmission. For those devices that can afford public key operations, they will use their public/private key pairs to establish session keys to encrypt the data exchanged [25]. For those which cannot afford public key operation, either a key escrow or an initial key distribution phase will be introduced to set up the symmetric key sharing among the devices in a group-wise or pair-wise fashion.

Data privacy could be viewed as a form of "selective confidentially" granted by the data owner. We could let users/subject/caregiver to configure the access of their data. However, this is not enough since private information may indeed leak in an unintentional way. For example, the traffic data in a health center may already be de-indentified. However, if an attacker is equipped with an appropriate tracking algorithm and also obtains other types of information about a person, such as the type of room (e.g., bathroom) he is visiting at a certain time, he will be able to link a daily habit or activity with the data set and associate this with the actual corresponding person. While this type of information may be important to a doctor, it is not appropriate for a stranger. Therefore, there are two types of actions. First, to minimize the amount of information being collected to the essential amount needed to form an event. Secondly, we have to sanitize the collected data before we actually publish it or share it, even if it is aimed at general-purpose research. We will need to anonymize such a dataset to make it resistant to popular data mining methods. At the same time, we must also keep certain properties associated with the dataset in order for it to be valuable for further analysis. For example, we may wish to use the dataset to optimize the layout of the physical apartment space of a person and the associated sensors for data collection in order to schedule better services [13]. Thus, a delicate trade-off appears between having enough data to identify an event and, at the same time, reduce and protect the data against privacy invasion.

Data Availability: The availability is the basis of the confidentiality and integrity, and requires the data or service to be continuously available. The security required must provide intrusion detection and fault-tolerant-and-recover mechanisms, and work against attacks such as, Denial-of-Service (DoS) attacks. The resiliency is more critical in assistive applications since any network misconnection or dysfunction of the medical devices may endanger human lives.

5.2 High Level Security on Sensitive Events

After raw data is processed and transformed into events, a higher level of security should be provided to protect those events defined as sensitive. The mechanism we propose is to allow the subjects or family members to authorize the access of his/her events and to enforce the system to check the compliance when someone requests them. We propose to define *event access* using widely accepted Semantic Web standards such as OWL, RDF,

and XML. Figure 3 gives an example of the access description of a *bathroom-visit event*.

```
<owl:Class rdf:type=”#event”>
<owl:DataTypeProperty rdf:ID=”timestamp”/>
      <rdfs:domain rdf:resource="#time"/>
       <rdfs:range rdf:resource="&xsd;time"/>
<owl:DataTypeProperty rdf:ID=”location”/>
      ...
</owl>
<event id="8739173917">
<timestamp> 2009.2.18.12:50pm </timestamp>
      <location> x: xxxx; y: yyyy </location>
      <type> bathroom visit </type>
      <physical quantities type="hit">
      <dooropen newton> 5 </dooropen newton>
      <velocity> 4 m/h </velocity>
      <duration> 10 m </duration>
      </physical quantities>
</event>
<Rules>
      <Rule type="home">
      <condition type=”event”>
      <before> B ← all other events detected
      within 1 hour </before>
      <present> P ←  Newton > 10 v velocity >
      10 m/h v duration > 30m </present>
      </condition>
      <action> report injury ← P v (B =
      abnormal) </action>
      </Rule>
</Rules>
<Access>
<action> check role of requester R ←
Requester </action>
      <Access type="bathroom">
      <condition duration=”9a-5p”>
      <allowed> ALL(TRUE) </allowed>
      </condition>
      <condition duration=”6p-12a&12a-8a”>
      <allowed> Doctor(R) and Nurse(R)
      </allowed>
      </condition>
      <condition assistance=”robot”>
      <allowed> on call ← injury </allowed>
      <denied> video ← false </denied>
      </condition>
</Access>
```

Figure 3 Sensitive Event

This event is characterized by 3 or more parameters, such as, the type of force used to open the bathroom door, the walking speed to the bathroom door, and the duration of the bathroom visit. The *event access* description is to be executed when such an event has been requested. In this example, only doctors and nurses can see all such event records during the night. An assistive robot may be allowed to be on call in case there is an accident associated with this event.

5.3 Privacy vs. Emergency

Emergency situations may require immediate access to sensitive data in order to prevent harm. A good example is where someone's movements are highly unusual such as if they are being physically attacked. In a pervasive assistive environment, video is to be avoided because of privacy concerns. However, in case of emergency, video sensors might only be activated on demand to validate that an emergency is in fact occurring. In these cases, one possibility is to follow the approach in the Clinical Information System Security model [14] where access is allowed but where we enforce strict accountability, so abuses can be dealt with procedurally.

5.4 Data Mining Techniques and Privacy Information Leaking

The ACPS human activity datasets can be used to support many other research projects, such as the development of new types of data fusion algorithms. It is important that these datasets be protected, especially as they may be shared on a network. To preserve privacy, we sanitize or anonymize certain types of location data in an assistive environment [13,15], which means we remove any (human) identity information from the location data. However, careful consideration of this idea reveals that even reporting only raw location data without identities is not enough to protect the privacy of humans: because of the continuity of motion data, locations of a single human can be tracked using various algorithms, e.g., a tracking algorithm can accurately estimate the trajectory of a single human. Furthermore, if a human's trajectory goes through sensitive or identifiable places, an outsider might see this as private information and these places may also provide connections to a person's identity. Thus, we have the challenge of balancing the tradeoff between event identification accuracy and data anonymization.

We deploy methods from our previous work on sanitizing raw datasets to make them resilient against popular tracking methods such as Kalman filter methods [16], while still retaining properties for general purpose research such as traffic analysis to optimize the distribution of resources or placement of

utilities. We have designed and implemented a method called *Dynamic Mix Zones (DMZ)* to perturb location information efficiently in order to minimize the chance of it being abused to derive identity information [13]. The DMZ method creates path confusion by dynamically creating mix zones. Two metrics were used to evaluate performance: the *indistinguishability ratio* and the *anti-tracking ratio*. Compared with previous methods, since DMZ randomizes multiple objects at the same time, it has better performance on mixing location samples to prevent malicious tracking. Efforts are under way to improve this work with approximation algorithms to select Dynamic Mix Zones. This has been proven NP-complete and current approximation algorithms such as the one found in [17], approach this problem by trading off running time and approximation factors.

6. EVENT VISUALIZATION (ZSCOPE)

As part of our framework, there is a front-end *information visualization interface* (ZSCOPE) that summarizes a history of key current and past events taking place. We use a physical apartment testbed, the Heracleia Apartment (**HA**) (in Figure 4.) of the Human Centered Computing Laboratory, to perform simulations that evaluate device training. ZSCOPE will be used to help a human operator or user locate active devices, their function and priority and provide ways to interact with them. Ongoing empirical studies collect human activity data from HA in order to: (1) to understand needs for human assistance and how the devices and instruments could be involved; and (2) to track the visualization and training needs of human operators.

Figure 4 The Heracleia Apartment

ZSCOPE is also used to illustrate the interactive nature of the EI mechanism and the generated events regarding patient behavior, or worker performance and to provide an intuitive interface that can help a human understand how to control or modify his/her ACPS. The visualized events may tell whether the patient follows the medical instructions or how well such a caregiver performs his/her tasks in order to correct possible mistakes. ZSCOPE can be particularly useful in caregiver or user training regarding, for example, how to use new rehabilitation devices that were added, or provide indicators that predict risk or neglect.

An example of the tools that make up the ZSCOPE instrument can be seen in Figure 4.1. ZSCOPE has four main modules for interacting with the event driven environment: (a) Events, (b) the Digital Library, (c) the Data Broker, (d) Support, and (e) the Privacy and Security module. In the case of the Event module, ZSCOPE includes the *Event Detection* tool that records what is happening in the apartment and a Map tool that provides the visualization (layout) of the apartment, showing the location of sensors, thus indicating when and where each event is occurring.

The *Digital Library* module contains three main tools. The first tool is the library-building tool. The library is composed of case studies for different aspects of human behavior in an assistive living environment. The other two tools include a *browse and search function* of the digital library, and a set of *bookmarks* to related websites to the material. The *Data Broker* module allows users to share or restrict information with their peers. The Co-Op tool includes collaboration and negotiation mechanisms to share data. In addition, recommendations about the data and who supplies the data are scored and ranked.

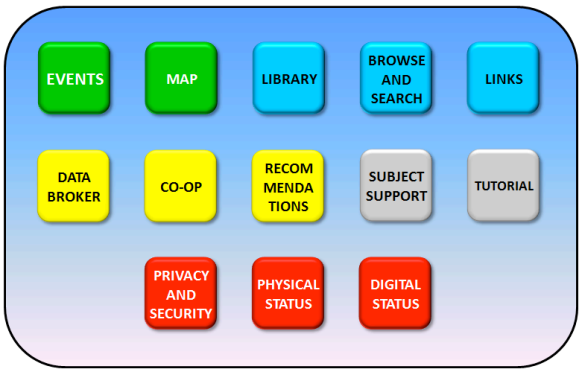

Figure 4.1 ZSCOPE interface example, showing the toolkits

No assistive system would be complete without a way to define the type of subject and how to provide help to the humans concerned. The ZSCOPE instrument includes a configuration module to allow the user to define a test subject or a patient, and an online tutorial to help a new user learn about the modules.

The Privacy and Security module tackles issues of maintaining anonymity and setting the preferences for privacy. It includes two troubleshooting tools as well. Sensors can be lost, run down on batteries, be broken, or even tampered with. These changes affect the security of the ACPS environment and would be listed as problems in a physical status report. These problems do not appear only in the physical world, either. The changing of a security key, or an odd delay or faster response from the system could indicate a problem with the routing or even an outside attack. So, the digital health of the system also has to be monitored and be available within the Privacy and Security module. The collection of these modules and their associated tools make up the ZSCOPE interface for an event driven system.

7. HEALTH EVALUATION FRAMEWORK

The *health evaluation fram*ework of an ACPS involves a new type of electronic health record that is able to automatically integrate behavior patterns with a person's medical condition, medication and symptoms (e.g., ways to connect fMRI brain changes with physical activity, heart function and new therapy). In our ACPS framework, events are designed to link to (synthetic) medical records, and the Event Identification mechanism is evaluated by using common normal individual difference variants. Large volumes of data from many individuals are integrated to define common or typical patterns of physiological and behavioral data.

Our previous results on fall and other event detection [4] are integrated in conjunction to variables such as, heart rate, blood pressure, eye movement, metabolic work demand, mood or affect, and compensatory movements to evaluation the effectiveness of the ACPS.

The evaluation framework includes metrics according to real-world applications, such as (a) how such detected patterns are changed with the use of common assistive walking devices; (b) what modifications users make as they become proficient in use of the device or as their health or fitness level changes; (c) what are common or typical changes in physiological and behavioral variables associated with aging; (d) are the patterns altered by the level of fitness, nutritional balance, mood or affect, or social engagement; (e) in what ways are these patterns altered by common acute and chronic health conditions; (f) are there changes that portend increased risk for acute health conditions; (g) under what conditions can these patterns be intentionally altered through medical therapies.

The health evaluation framework is of interest to actual healthcare providers. ACPS gives them tools to identify typical physiological and behavioral patterns associated with various health conditions and social and genetic variations.

8. RELATED WORK

CPS design challenges appear in [18]. Gabor et al. connect correct design to safety- or business-critical contexts, and propose a model-integrated development of CPS [19]. Network QoS management is discussed in [20] where Feng et.al discuss the network QoS challenge for a successful CPS. Albert in [21] discusses CPS issues in medical applications. Lui et al. review issues with providing care to the elderly population in

[22] and raise warnings about the non-sustainability of the Social Security and Medicare/Medicaid systems. In [23], CPS used in health-care of the elderly might combine packaged sensors with a data streaming service and network protocols. A network enabled real-time embedded database in [24] collects data using wireless sensors in a CPS system.

9. CONCLUSIONS

This paper proposed an event identification (EI) framework with a multi-level data to knowledge approach on multimodal human activity data in complex physical pervasive environments, converting low level data semantics to high level, with privacy and security built-in. It provided a multi-level security and privacy framework. It also provided an integrated information visualization interface called ZSCOPE that illustrates relations among the events, a subject, and the environment.

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. This work is supported in part by the National Science Foundation under award number CT-ISG 0716261. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] Zhengyi Le, Matt Bishop, and Fillia Makedon, Strong Mobile Device Protection from Loss and Capture Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'09), Corfu, Greece, June 9-13, 2009.

[2] Alan Bowling, Zhengyi Le, and Fillia Makedon, SAL: A simulation and analysis tool for assistive living environments Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'09), Corfu, Greece, June 9-13, 2009.

[3] Kyungseo Park, Eric Becker, Jyothi K. Vinjumur, Zhengyi Le, and Fillia Makedon, Human Behavioral Detection and Data Cleaning in Assisted Living Environment using Wireless Sensor Networks Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'09), Corfu, Greece, June 9-13, 2009.

[4] Eric Becker, Zhengyi Le, Kyungseo Park, Yong Lin, and Fillia Makedon, Event-based Experiments in an Assistive Environment using Wireless Sensor Networks and Voice Recognition Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'09), Corfu, Greece, June 9-13, 2009.

[5] Eric Becker, Gutemberg Guerra-Filho, and Fillia Makedon, Automatic Sensor Placement in a 3D Volume Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'09), Corfu, Greece, June 9-13, 2009.

[6] Eric Becker, Vangelis Metsis, Roman Arora, Jyothi Vinjumur, Yurong Xu, Fillia Makedon, SmartDrawer: RFID-Based Smart Medicine Drawer for Assistive Environments Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'09), Corfu, Greece, June 9-13, 2009.

[7] Yong Lin, Eric Becker, Kyungseo Park, Zhengyi Le, Fillia Makedon, Decision Making in Assistive Environments using Multimodal Observations Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'09), Corfu, Greece, June 9-13, 2009.

[8] Roman Arora, Vangelis Metsis, Rong Zhang and Fillia Makedon, Providing QoS in Ontology Centered Context Aware Pervasive Systems Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'09), Corfu, Greece, June 9-13, 2009.

2008

[9] Eric Becker, Yurong Xu, Steven Ledford, Fillia Makedon, A wireless sensor network architecture and its application in an assistive environment Proceedings of the 1st International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'08), Athens, Greece, July 16-18, 2008.

[10] Eric Becker, Yurong Xu, Heng Huang, Fillia Makedon, Requirements for implementation of localization into real-world assistive environments Proceedings of the 1st International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'08), Athens, Greece, July 16-18, 2008.

[11] Vangelis Metsis, Zhengyi Le, Yu Lei, and Fillia Makedon, Towards An Evaluation Framework for

Assistive Environments Proceedings of the 1st International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'08), Athens, Greece, July 16-18, 2008.
[12] Zhengyi Le, Yi Ouyang, Yurong Xu, and Fillia Makedon, Mobile Device Protection against Loss and Capture Proceedings of the 1st International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'08), Athens, Greece, July 16-18, 2008.
[13] Yi Ouyang, Yurong Xu, Zhengyi Le, Guanling Chen, and Fillia Makedon, Providing Location Privacy in Assisted Living Environments Proceedings of the 1st International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'08), Athens, Greece, July 16-18, 2008.
[14] R. Anderson, "A Security Policy Model for Clinical Information Systems," Proceedings of the 1996 IEEE Symposium on Security and Privacy, pp. 34–48, May 1996.
[15] R. Crawford, M. Bishop, B. Bhumiratana, L. Clark, and K. Levitt, "Sanitization Models and their Limitations," Proceedings of the New Security Paradigms Workshop, pp. 41–56, Sep. 2006.
[16] J. Durbin and S. J. Koopman, "Time Series Analysis by State Space Methods," Oxford University Press Inc, New York 2001.
[17] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005.
[18] E. A. Lee, "Cyber physical systems: Design challenges," ISORC, IEEE Computer Society, pp. 363-369, 2008.
[19] G. Karsai and J. Sztipanovits, "Model-integrated development of cyber-physical systems. In Software Technologies for Embedded and Ubiquitous Systems,," 6th IFIP WG 10.2 International Workshop, SEUS 2008, Anacarpi, Capri Island, Italy, vol. 5287, pp. 46-54, Springer, 2008.
[20] F. Xia, L. Ma, J. Dong, and Y. Sun, " Network qos management in cyber-physical systems," ICESSSYMPOSIA '08: Proceedings of the 2008 International Conference on Embedded Software and Systems Symposia, pp. 302-307, Washington, DC, USA, IEEE Computer Society, 2008.
[21] A. M. K. Cheng, "Cyber-physical medical and medication systems," ICDCSW '08: Proceedings of the 2008 The 28th International Conference on Distributed Computing Systems Workshops, pp. 529-532, Washington, DC, USA, 2008.
[22] L. Sha, G. S., X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC '08. IEEE International Conference, pp. 1-9, 2008.
[23] A. D. Wood and J. A. Stankovic, "Human in the loop: distributed data streams for immersive cyber-physical systems," SIGBED Rev, vol. 5, pp. 1-2, 2008.
[24] K.-D. Kang and S. H. Son, "Real-time data services for cyber physical systems," 1st International Workshop on Cyber-Physical Systems(1st WCPS'08) at 28th IEEE International Conference on Distributed Computing Systems (28th ICDCS'08), Beijing, China, June 2008.
[25] Zhengyi Le, Yi Ouyang, Yurong Xu, James Ford, and Fillia Makedon, "Preventing Unofficial Information Propagation", Proceedings of the 9th International Conference on Information and Communication Security (ICICS'07), LNCS, Springer, pp. 113-125, 2007.
[26] H. Huang and C. Ding, "Robust Tensor Factorization Using R1 Norm," IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2008), pp. 1-8, 2008.
[27] C. Ding, H. Huang, and D. Luo, "Tensor Reduction Error Analysis -- Applications to Video Compression and Classification," IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2008), pp. 1-8, 2008.
[28] H. Huang, C. Ding, D. Luo, and T. Li, "Simultaneous Tensor Subspace Selection and Clustering: The Equivalence of High Order SVD and K-Means Clustering," The 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 2008), pp. 327-335, 2008.