ARTICLE IN PRESS
JID: COMPNW [m3Gdc;February 21, 2017;13:55]

Computer Networks xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Editorial

Cyber–physical systems and context-aware sensing and computing

1. Introduction

Cyber–physical systems (CPS) involve the integration of real-world physical systems and processes with the virtual (cyber) world. The interaction between physical processes and the cyber world occurs in a feedback loop, with information flowing back and forth. The embedded devices and networks monitor and control the physical processes and systems, and the physical processes in turn influence the computation. CPS can be applied across many industries such as management and maintenance of critical infrastructure like bridges and roadways; remote patient healthcare systems; intelligent traffic management and automated vehicles in transportation; energy production, distribution and optimization through smart grids and smart buildings; robotic machinery and computer-controlled actuation in manufacturing.

CPS applications are expected to deliver various critical services. Being able to sense the physical environment and adapt accordingly will ensure that not just any service is delivered at any time, but the proper services are delivered at the correct time. Through context-aware sensing and computation, the CPS can acquire contextual information and use it intelligently. These systems will thus be able to anticipate needs and situations and react to the environment around them.

The purpose of this special issue is to bring together studies proposing novel techniques, algorithms, frameworks, models, and solutions to address challenges such as interoperability, security, and infrastructure associated with CPS and context aware sensing.

We accepted seven articles after two review rounds consisting of three reviews from experts in the different areas. The special issue contains seven papers organized in the following categories: (i) Visual surveillance, (ii) Security in the smart grid, (iii) Energy disaggregation, (iv) Context-aware prediction, (v) Clustering in wireless sensor networks, and (vi) Transportation.

The first part of this special issue is devoted to "*Quantum-Inspired Algorithm for Cyber–Physical Visual Surveillance*" which presents a novel algorithm, namely; the Quantum-inspired Tabu Search algorithm with Entanglement (QTSwE) which is based on the Quantum-inspired Tabu Search (QTS) algorithm and the quantum entanglement feature. The goal is building optimal network topologies.

Two areas where this algorithm can be useful are traffic control and surveillance systems. The article highlights aspects of network deployment as a critical issue in Wireless Sensor Networks and Cyber–Physical Systems (WSN/CPS). Their implementation further indicates how effectively their algorithm is applied in order to solve problems such as determining the minimum number of sensors as well as their location as opposed to heuristic and deterministic approaches which have been used before to tackle these problems. Shu-Yu Kuo et al. further indicate that a local search was used to improve the ability of the QTS algorithm, wherein the QTS part is used to find better solutions. After applying their proposed approach, experimental results show that for real applications, QTSwE reveals powerful search capabilities as well as providing means for solving deployment problems with high dependency. Thus, an overall improvement is realized in terms of deployment, whereby entanglement methods together with QTS are used to get the first topology as well as finding feasible solutions by means of applying quantum linear superposition and the tabu search, such that the searching speed is also enhanced. In conclusion, their results indicate that, QTSwE provides better performance than other heuristic and deterministic strategies which have been applied in an effort to solve deployment problems. Most importantly, their work shows that QTSwE can be used to build network topologies with a minimum number of sensors as well as ensuring network connectivity using less computational complexity.

The next part of the special issue addresses challenges experienced in securing smart grid metering sys-

http://dx.doi.org/10.1016/j.comnet.2017.02.012
1389-1286/

tems where fraudsters tamper with these meters to register incorrect consumption or usage readings. This phenomenon is called Non-Technical Loss (NTL). This paper discusses the new form of smart meter fraud called Colluded Non-Technical Loss (CNTL) fraud which is difficult for meter fraud detection schemes to detect, since multiple fraudsters can concur or cooperate to commit the fraud. This paper by Wenlin Han et al. proposes a novel method for detecting CNTL fraud since existing detection schemes struggle to differentiate between co-existing or collaborating fraudsters. Their proposed method uses recursive least squares to quickly detect tampered meters and apply a mathematical model to detect different fraudsters. To test their detection method, they introduced potential types of frauds which have been previously discovered on the smart grid. They categorized fraud into four different types namely: segmented CNTL frauds, fully overlapped CNTL frauds, partially overlapped CNTL frauds and lastly combined CNTL frauds. This paper further proposes a novel detector called Colluded Not-Technical Loss Fraud Detection (CNFD) whose main purpose is to solve the issue of CNTL experienced in smart grids. Their proposed detection method—CNFD—has two distinct steps which it uses to detect CNTL frauds, namely; NTL fraud detection and fraudster differentiation. Their proposed detection method can effectively detect a tampered meter within a group of these meters as well as detect multiple fraudsters on the tampered meter. Their experimental results show that CNFD can effectively detect all four types of meter frauds indicated above.

Another paper in this part, "A privacy-aware Data Dissemination Scheme for Smart Grid with Abnormal Data Traceability", is based on bilinear group theory and non-interactive zero-knowledge proof and is used for data privacy preservation. Xu Zhang et al. clearly demonstrate that the proposed scheme will bring advantages to smart grids in terms of preserving data integrity and customer identity privacy. Moreover, the paper tackles data privacy and abnormal data detection and tracing at the same time. Their implementation further indicates how their scheme effectively addresses abnormal data detection and tracing by making use of a novel group signature technique. A link function was designed to determine whether a user has different signatures signed to minimize the time and transmission overhead for tracing. In conclusion, they applied solid security analysis to confirm that the proposed scheme achieves source authentication, signature anonymity, and signature unforgeability from both external and internal attacks, data traceability and link-ability. The performance of the proposed scheme was compared with already existing counterparts and proven to be efficient.

The third part of the issue addresses the challenges of energy usage in terms of occupancy-aided energy disaggregation for apartments with typical household appliances. This paper uses an energy disaggregation technique to identify the sources of high energy utilization in households without introducing extra meter costs. Their work provides motivation to users on how to take proper measures for energy saving as well as facilitate demand response programs for efficient energy utilization. The paper proposes an occupancy-aided energy disaggregation (OAED) approach as a strategy to minimize the computational complexity of pure energy disaggregation. This strategy is applied in terms of occupancy information, wherein time intervals for occupied and unoccupied periods are classified. It introduces the OAED framework based on non-intrusive occupancy detection for residential households, whereby this framework generally depicts the possibility of leveraging occupation information in the process of energy disaggregation. To measure how high energy utilization for residential households is incurred, they focus on time intervals when there is occupation, whereas the minimum energy consumption estimation can be easily performed for unoccupied intervals. As an effort to disaggregate energy from multiple household appliances, Guoming Tang et al. adopt two different energy disaggregation techniques namely; the signature based approach using least square estimation (LSE) and the state transition based approach which applies the Hidden Markov Model (HMM). Their experimental results indicate that the OAED approach can significantly reduce the computational complexity with good accuracy in energy disaggregation.

The fourth part of the issue deals with *Context-Aware Prediction of Access Points Demand*. This work predicts the number of network sessions established at access points of a Wi-Fi network based on the behavior of users. The paper presents a methodology based on the application of Matrix Factorization (MF) and gradient decent and also highlights another context-aware aspect other than the physical context (i.e. hardware) which is human behavior. They show that human behavior can have an influence in network enhancement and maintenance as the demand of sufficient Access Points (APs) based on user behavior may suggest locating some elements of the network elsewhere. To enhance their prediction model, they apply existing techniques that provide good prediction results especially with systems where user behavior and preference have greater influence namely; the Recommender Systems (RS) and the Predicting Student Performance (PSP) algorithms. To validate their prediction model, they follow a methodology which is composed of three phases namely; (a) Collecting data about sessions established by users in APs, (b) the Prediction—where the behavior of the incomplete network with a performance matrix is built using real network data, and (c) the Validation—where quality of predictions is validated by comparing them with real performance of the incomplete network. Their experimental results show that using real and predicted data in a university environment, it is possible to achievement consistent, valid approaches which can be successfully applied in wireless networks considering users' preferences for usual activities.

The fifth part of the special issue discusses Dynamic Clustering and management of Mobile Wireless Sensor Networks. This is where a self-organizing and adaptive Dynamic Clustering Mobile Data Collector solution divides the network into groups of cooperating clusters. The paper points out the advantages of network clustering. It also indicates the role that the clusters, called service zone, play in the reduction of signaling and energy consumption and resource utilization. Furthermore, the advantages of grouping sensor nodes into small clusters with regards to energy consumption and buffering are indicated. In conclusion,