Neural translation

ASSURED: Architecture for Secure Software Update of Realistic Embedded Devices

Secure firmware update is an important stage in the IoT device life-cycle. Prior techniques, designed for other computational settings, are not readily suitable for IoT devices, since they do not consider idiosyncrasies of a realistic large-scale IoT deployment. This motivates our design of ASSURED, a secure and scalable update framework for IoT. ASSURED includes all stakeholders in a typical IoT update ecosystem, while providing end-to-end security between manufacturers and devices. To demonstrate its feasibility and practicality, ASSURED is instantiated and experimentally evaluated on two commodity hardware platforms. Results show that ASSURED is considerably faster than current update mechanisms in realistic settings.  
 **main\_author: Gene Tsudik**  
 **published\_date: 2018-07-13 11:00:00+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1807.05002v1*

TDOA-based Localization via Stochastic Gradient Descent Variants

Source localization is of pivotal importance in several areas such as wireless sensor networks and Internet of Things (IoT), where the location information can be used for a variety of purposes, e.g. surveillance, monitoring, tracking, etc. Time Difference of Arrival (TDOA) is one of the well-known localization approaches where the source broadcasts a signal and a number of receivers record the arriving time of the transmitted signal. By means of computing the time difference from various receivers, the source location can be estimated. On the other hand, in the recent few years novel optimization algorithms have appeared in the literature for $(i)$ processing big data and for $(ii)$ training deep neural networks. Most of these techniques are enhanced variants of the classical stochastic gradient descent (SGD) but with additional features that promote faster convergence. In this paper, we compare the performance of the classical SGD with the novel techniques mentioned above. In addition, we propose an optimization procedure called RMSProp+AF, which is based on RMSProp algorithm but with the advantage of incorporating adaptation of the decaying factor. We show through simulations that all of these techniques---which are commonly used in the machine learning domain---can also be successfully applied to signal processing problems and are capable of attaining improved convergence and stability. Finally, it is also shown through simulations that the proposed method can outperform other competing approaches as both its convergence and stability are superior.  
 **main\_author: Sonia Heemstra de Groot**  
 **published\_date: 2018-07-12 21:13:51+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1807.04824v1*

Joint Status Sampling and Updating for Minimizing Age of Information in the Internet of Things

The effective operation of time-critical Internet of things (IoT) applications requires real-time reporting of fresh status information of underlying physical processes. In this paper, a real-time IoT monitoring system is considered, in which the IoT devices sample a physical process with a sampling cost and send the status packet to a given destination with an updating cost. This joint status sampling and updating process is designed to minimize the average age of information (AoI) at the destination node under an average energy cost constraint at each device. This is formulated as an infinite horizon average cost constrained Markov decision process (CMDP) and transformed into an unconstrained MDP using a Lagrangian method. For the single IoT device case, the optimal policy for the CMDP is shown to be a randomized mixture of two deterministic policies for the unconstrained MDP, which is of threshold type. Then, a structure-aware optimal algorithm to obtain the optimal policy of the CMDP is proposed and the impact of the wireless channel dynamics is studied while demonstrating that channels having a larger mean channel gain and less scattering can achieve better AoI performance. For the case of multiple IoT devices, a low-complexity distributed suboptimal policy is proposed with the updating control at the destination and the sampling control at each device. Then, an online learning algorithm is developed to obtain this policy, which can be implemented at each IoT device and requires only the local knowledge and small signaling from the destination. The proposed learning algorithm is shown to converge almost surely to the suboptimal policy. Simulation results show the structural properties of the optimal policy for the single IoT device case; and show that the proposed policy for multiple IoT devices outperforms a zero-wait baseline policy, with average AoI reductions reaching up to 33%.  
 **main\_author: Walid Saad**  
 **published\_date: 2018-07-11 21:21:08+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1807.04356v1*

Using Topic Models to Mine Everyday Object Usage Routines Through Connected IoT Sensors

With the tremendous progress in sensing and IoT infrastructure, it is foreseeable that IoT systems will soon be available for commercial markets, such as in people's homes. In this paper, we present a deployment study using sensors attached to household objects to capture the resourcefulness of three individuals. The concept of resourcefulness highlights the ability of humans to repurpose objects spontaneously for a different use case than was initially intended. It is a crucial element for human health and wellbeing, which is of great interest for various aspects of HCI and design research. Traditionally, resourcefulness is captured through ethnographic practice. Ethnography can only provide sparse and often short duration observations of human experience, often relying on participants being aware of and remembering behaviours or thoughts they need to report on. Our hypothesis is that resourcefulness can also be captured through continuously monitoring objects being used in everyday life. We developed a system that can record object movement continuously and deployed them in homes of three elderly people for over two weeks. We explored the use of probabilistic topic models to analyze the collected data and identify common patterns.  
 **main\_author: Hayley Hung**  
 **published\_date: 2018-07-11 20:30:44+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1807.04343v1*

ThingPot: an interactive Internet-of-Things honeypot

The Mirai Distributed Denial-of-Service (DDoS) attack exploited security vulnerabilities of Internet-of-Things (IoT) devices and thereby clearly signalled that attackers have IoT on their radar. Securing IoT is therefore imperative, but in order to do so it is crucial to understand the strategies of such attackers. For that purpose, in this paper, a novel IoT honeypot called ThingPot is proposed and deployed. Honeypot technology mimics devices that might be exploited by attackers and logs their behavior to detect and analyze the used attack vectors. ThingPot is the first of its kind, since it focuses not only on the IoT application protocols themselves, but on the whole IoT platform. A Proof-of-Concept is implemented with XMPP and a REST API, to mimic a Philips Hue smart lighting system. ThingPot has been deployed for 1.5 months and through the captured data we have found five types of attacks and attack vectors against smart devices. The ThingPot source code is made available as open source.  
 **main\_author: Fernando Kuipers**  
 **published\_date: 2018-07-11 13:09:25+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1807.04114v1*

Internet of Things: Infrastructure, Architecture, Security and Privacy

Internet of Things (IoT) is one of the emerging technologies of this century and its various aspects, such as the Infrastructure, Security, Architecture and Privacy, play an important role in shaping the future of the digitalised world. Internet of Things devices are connected through sensors which have significant impacts on the data and its security. In this research, we used IoT five layered architecture of the Internet of Things to address the security and private issues of IoT enabled services and applications. Furthermore, a detailed survey on Internet of Things infrastructure, architecture, security, and privacy of the heterogeneous objects were presented. The paper identifies the major challenge in the field of IoT; one of them is to secure the data while accessing the objects through sensing machines. This research advocates the importance of securing the IoT ecosystem at each layer resulting in an enhanced overall security of the connected devices as well as the data generated. Thus, this paper put forwards a security model to be utilised by the researchers, manufacturers and developers of IoT devices, applications and services.  
 **main\_author: Mahdi H. Miraz**  
 **published\_date: 2018-07-11 11:45:18+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1807.04087v1*

Knowledge Extracted from Recurrent Deep Belief Network for Real Time Deterministic Control

Recently, the market on deep learning including not only software but also hardware is developing rapidly. Big data is collected through IoT devices and the industry world will analyze them to improve their manufacturing process. Deep Learning has the hierarchical network architecture to represent the complicated features of input patterns. Although deep learning can show the high capability of classification, prediction, and so on, the implementation on GPU devices are required. We may meet the trade-off between the higher precision by deep learning and the higher cost with GPU devices. We can success the knowledge extraction from the trained deep learning with high classification capability. The knowledge that can realize faster inference of pre-trained deep network is extracted as IF-THEN rules from the network signal flow given input data. Some experiment results with benchmark tests for time series data sets showed the effectiveness of our proposed method related to the computational speed.  
 **main\_author: Takumi Ichimura**  
 **published\_date: 2018-07-11 05:37:02+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1807.03954v1*

Blockchain-based PKI for Crowdsourced IoT Sensor Information

The Internet of Things is progressively getting broader, evol-ving its scope while creating new markets and adding more to the existing ones. However, both generation and analysis of large amounts of data, which are integral to this concept, may require the proper protection and privacy-awareness of some sensitive information. In order to control the access to this data, allowing devices to verify the reliability of their own interactions with other endpoints of the network is a crucial step to ensure this required safeness. Through the implementation of a blockchain-based Public Key Infrastructure connected to the Keybase platform, it is possible to achieve a simple protocol that binds devices' public keys to their owner accounts, which are respectively supported by identity proofs. The records of this blockchain represent digital signatures performed by this Keybase users on their respective devices' public keys, claiming their ownership. Resorting to this distributed and decentralized PKI, any device is able to autonomously verify the entity in control of a certain node of the network and prevent future interactions with unverified parties.  
 **main\_author: Hugo Sereno Ferreira**  
 **published\_date: 2018-07-10 21:08:13+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1807.03863v1*

Tensorized Spectrum Preserving Compression for Neural Networks

Modern neural networks can have tens of millions of parameters, and are often ill-suited for smartphones or IoT devices. In this paper, we describe an efficient mechanism for compressing large networks by {\em tensorizing\/} network layers: i.e. mapping layers on to high-order matrices, for which we introduce new tensor decomposition methods. Compared to previous compression methods, some of which use tensor decomposition, our techniques preserve more of the networks invariance structure. Coupled with a new data reconstruction-based learning method, we show that tensorized compression outperforms existing techniques for both convolutional and fully-connected layers on state-of-the art networks.  
 **main\_author: Furong Huang**  
 **published\_date: 2018-05-25 20:21:50+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1805.10352v2*

Dynamic Allocation of Serverless Functionsin IoT Environments

The IoT area has grown significantly in the last few years and is expected to reach a gigantic amount of 50 billion devices by 2020. The appearance of serverless architectures, specifically highlighting FaaS, raises the question of the of using such in IoT environments. Combining IoT with a serverless architectural design can be effective when trying to make use of the local processing power that exists in a local network of IoT devices and creating a fog layer that leverages computational capabilities that are closer to the end-user. In this approach, which is placed between the device and the serverless function, when a device requests for the execution of a serverless function will decide based on previous metrics of execution if the serverless function should be executed locally, in the fog layer of a local network of IoT devices, or if it should be executed remotely, in one of the available cloud servers. Therefore, this approach allows to dynamically allocating functions to the most suitable layer.  
 **main\_author: Hugo Sereno Ferreira**  
 **published\_date: 2018-07-10 16:59:01+00:00**  
 *pdf\_url: http://arxiv.org/pdf/1807.03755v1*