The 29th Biennial Symposium on Communications (BSC 2018) Final Program

Wednesday, June 6, 2018 to Thursday, June 7, 2018. Times listed in Eastern Time (US & Canada). All talks are held in the lower floor of the Engineering Building (245 Church Street)

Wednesday, June6, 2018

9:00 am – 10:am (ENG-LG04) Keynote Presentation, Aria Nosratinia (UT Dallas):" Coherence Diversity: a new source of gains in wireless networks"

Session Chair: Ali Miri (Ryerson)

Abstract: Due to differences in mobility and local scattering, the links in a wireless network can experience disparities in coherence time that, in the past, were mostly ignored in the modeling and analysis of networks. We show that these coherence disparities can be a source of capacity gains (denoted "coherence diversity") that are distinct and independent from classical gains such as spatial multiplexing, beamforming, and multiuser diversity. A product superposition is introduced that can exploit these differences in coherence and yield gains in degrees of freedom. The gains are an increasing function of the mismatch in coherence times and vanish in the absence of coherence disparity. Coherence diversity will be explored in the context of pilot-based as well as Grassmannian communication. It is shown that differences in coherence bandwidth also yield a similar gain. Time permitting, non-uniformity of CSIT under coherence disparity and disparity in spatial coherence will be discussed. Several open problems in the broad area of coherence diversity will be highlighted.

10:00am – 10:20am Coffee Break

10:20 am – 12:00 pm (ENG-LG04) Session 1: Multiple Antenna Systems

Session Chair: Julian Cheng (UBC)

- 'A New Look at Optimum Macro Base Station Deployment in Heterogeneous Massive MIMO Networks for Eliminating Interference', Noha Hassan and Xavier Fernando

Heterogeneous networks (HetNets) offer a practical representation for 5G systems due to the recent trend of viewing the communication system as three dimensional (3D) with various slices cooperating among each other. Each slice represents a unique tier that has its own Base stations (BS) and serving users (UEs). Also, data can be transmitted among tiers, and UEs have the flexibility to switch between various tiers. In order to present the randomization that imposes such systems, a Poisson point process (PPP) has been widely used by default to allocate BSs and UEs in various tiers. However, the suggested locations are not the best ones to improve network performance and reduce interference. In this paper, we develop a new algorithm to find the optimum locations of Macro BSs in HetNets where every Macro BS along with its associate Micro BSs can be treated as an independent unit after eliminating interference from neighboring Macro and Micro BSs. The simulation results proved the validity of our approach and the promising enhancement to system performance.

- ‘Transmit Antenna Selection for Rank-deficient Spatial Multiplexing Systems’, Mohammad Kazem Izadinasab and Mohamed Oussama Damen

  In this work, we study a diversity optimal transmit antenna selection for rank-deficient spatial multiplexing (SM) systems with linear or decision-feedback (DF) receivers based on the fixed-complexity sphere decoder (FSD) ordering. We propose a regularized FSD (RFSD) transmit antenna selection algorithm by utilizing the regularized (or augmented) channel matrix in order to alleviate the rank-deficiency of the Gram channel matrix. In each iteration of the RFSD algorithm, one column of the channel corresponding to the row of the pseudo-inverse of the regularized channel matrix with the maximum norm is zeroed until L columns remain for transmission. The diversity optimality of the proposed technique is investigated by analysis and some computer simulations.

- ‘Updating Beamformers to Respond to Changes in Users’, Mostafa Medra, Andrew Eckford and Raviraj Adve

  We consider a multi-user multiple-input single-output downlink system that provides each user with a prespecified level of quality-of-service. The base station (BS) designs the beamformers so that each user receives a certain signal-to-interference-and-noise ratio (SINR). In contrast to most of the available literature in the beamforming field, we focus on the required modifications when the system changes. We specifically study three cases: (i) user entering the system, (ii) user leaving the system, and (iii) a change in the SINR target. We do so in order to avoid designing the entire system from scratch for every change in the requirements. In each of the three cases, we describe the modifications required to the beamforming directions and the power loading. We consider maximum ratio transmission (MRT), zero-forcing (ZF) and the optimal beamformers. The proposed modifications provide performance that is either exact or very close to that obtained when we redesign the entire system, while having much lower computational cost.

- ‘On the Error Performance of Space-Time Codes over MIMO Nakagami Fading Channels with Blockage’, Ahmed Aboutaleb, Wael Fatnassi, Zouheir Rezki and Anas Chaaban

  In this paper, we derive a closed-form upper bound on the error performance of space-time codes over Nakagami-m fading channels. Our upper bound is based on the pairwise error probability (PEP). We then examine the resulting diversity and coding gains to propose design criteria that maximize these gains. Orthogonal space-time block codes are shown to achieve the maximum diversity gain but not the maximum coding gain. Indeed, we show that there exists a trade-off between the diversity gain and the coding gain. Furthermore, we investigate the effect of blockage on the error performance using stochastic geometry. Our analysis and simulations show that blockage only reduces the coding gain and does not affect the diversity gain. This reduction in the coding gain is a function of the probability of line-of-sight (LOS) communication, path loss exponents, the distance between transceivers, and the coding gain without considering the effect of blockage. For instance, in a typical indoor environment, blockage due to humans or other obstacles can reduce the coding gain by up to 1.5 dB for a bit error probability of 10^{-3}.

- ‘A Hierarchical Graph Signal Processing Approach to Inference from Spatiotemporal Signals’, Nafiseh Ghoroghchian, Stark C. Draper and Roman Genov

Motivated by the emerging area of graph signal processing (GSP), we introduce a novel method to draw inference from spatiotemporal signals. Data acquisition in different locations over time is seen in sensor networks for diverse applications, from object tracking to electroencephalography (EEG) signal processing. In this paper we leverage novel techniques of GSP to extract spatiotemporal signals from such data sets.We develop a hierarchical feature extraction approach by mapping the data onto a series of spatiotemporal graphs. Such a model maps signals onto vertices of a graph and the time-space dependencies among signals are modeled by the edges weights.Signal components acquired from different locations and time often have complicated functional dependencies. Accordingly, their corresponding graph weights are learned from data and used in two ways. First, they are used as a part of the embedding related to the topology of graph such as density. Second, they provide the connectivities of the base graph for extracting higher level GSP-based features. The latter include the energies of graph Fourier transform in different frequency bands. We test our approach on the iEEG data set of the Kaggle seizure detection contest. In comparison to the winning code, the results show a slight net improvement and up to 6 percent improvement in per subject analysis, while the number of features are decreased by 75 percent on average.

12:00pm - 2:00pm Lunch

2:00pm – 5:00pm (ENG-LG04) Tutorial, Zheshen Zhang (Arizona):"Quantum Communications: Fundamentals, Applications, and Physical Realizations"

Abstract: Quantum information science gives rise to new communication paradigms that would offer unmatched security and capacity. This tutorial will provide an overview of the principles and applications of quantum communications. It will be comprised of three Sections: in Section I, we will introduce the basics of quantum information, i.e., how information is represented at a quantum mechanical level. The focus will be on the fundamental disparities between quantum and classical information, including the quantum superposition principle, measurement uncertainty, the no-cloning theorem, and quantum entanglement. In Section II, we will build upon the knowledge acquired in Section I to construct quantum-communication protocols that offer functionalities beyond the reach of classical communications. We will study quantum key distribution, quantum teleportation, entanglement swapping, and super-dense coding. Section III will be dedicated to bridging the gap between theory and experiment, by introducing the physical realizations of entanglement generation, operations and measurements on the quantum states of light, along with a case study of a complete quantum-communication system. The attendees of the tutorial are anticipated to learn the essential elements of quantum communications, from both theoretical and experimental perspectives. We hope that the materials presented in this tutorial will help to build connections between quantum and classical communications so that their respective tools and techniques may benefit each other to create new routes for interdisciplinary research.

5:00pm – 6:00pm (ENG-LG21) CSIT Meeting

6:30pm – 8:30pm Banquet

Thursday, June7, 2018

9:00am – 10:20am (ENG-LG04) Session 2a: Source Coding and Quantizer

Session Chair: Fady Alajaji (Queens)

- 'Binary CEO Problem under Log-Loss with BSC Test-Channel Model', Mahdi Nangir, Reza Asvadi, Mahmoud Ahmadian-Attari and Jun Chen

  In this paper, we propose an efficient coding scheme for the two-link binary Chief Executive Officer (CEO) problem under logarithmic loss criterion. The exact rate-distortion bound for a two-link binary CEO problem under the logarithmic loss has been obtained by Courtade and Weissman. We propose an encoding scheme based on compound LDGM-LDPC codes to achieve the theoretical bounds. In the proposed encoding, a binary quantizer using LDGM codes and a syndrome-coding employing LDPC codes are applied. An iterative joint decoding is also designed as a fusion center. The proposed CEO decoder is based on the sum-product algorithm and a soft estimator.

- 'Design of Optimal Entropy-constrained Successively Refinable Unrestricted Polar Quantizer for Bivariate Circularly Symmetric Sources', Huihui Wu and Sorina Dumitrescu

  This paper focuses on the design of entropy-constrained successively refinable unrestricted polar quantizer (EC-SRUPQ) for bivariate circularly symmetric sources. The proposed algorithm is globally optimal under the constraint that the magnitude quantizers' thresholds are confined to finite sets. The optimization problem is formulated as the minimization of a weighted sum of distortions and entropies. The proposed solution consists of a series of steps including solving the minimum-weight path problem for multiple node pairs in certain weighted directed acyclic graphs. The asymptotical time complexity is $O(K_1K_2^2P_{max})$, where K_1 and K_2 are the sizes of the sets of possible magnitude thresholds of the coarse

UPQ and refined UPQ, respectively, while P_{max} is the maximum number of phase levels in any phase quantizer of the coarse UPQ.

- 'Optimal Design of A Two-stage Wyner-Ziv Scalar Quantizer with Degraded Side Information', Qixue Zheng and Sorina Dumitrescu

  This work addresses the optimal design of a two-stage Wyner-Ziv scalar quantizer with degraded side information (SI). We assume that binning is performed optimally and address the design of the nested quantizer partitions. The optimization problem is formulated as minimizing a weighted sum of distortions and rates. The proposed solution algorithm is globally optimal when the source and SI are discrete, while the partition cells are contiguous. The algorithm is based on solving the single source or the all-pairs minimum-weight path problem in certain weighted directed acyclic graphs. A so-called partial Monge property is additionally introduced and a faster solution algorithm exploiting this property is proposed. Experimental results assess the practical performance of the proposed scheme.

- 'Successive Wyner-Ziv Coding for the Binary CEO Problem under Log-Loss', Mahdi Nangir, Reza Asvadi, Mahmoud Ahmadian-Attari and Jun Chen

  An l-link binary CEO problem is considered in this paper. We present a practical encoding and decoding scheme for this problem employing the graph-based codes. A successive coding scheme is proposed for converting an l-link binary CEO problem to the $(2l-1)$ single binary Wyner-Ziv (WZ) problems. By using the compound LDGM-LDPC codes, the theoretical bound of each binary WZ is asymptotically achievable. Our proposed decoder successively decodes the received data by employing the well-known Sum-Product (SP) algorithm and leverages them to reconstruct the source. The sum-rate distortion performance of our proposed coding scheme is compared with the theoretical bounds under the logarithmic loss (log-loss) criterion.

9:00am - 10:20am (ENG-LG21) Session 2b: Communication theory and energy harvesting
Session Chair: Andrew Eckford (York)

- 'Analysis of Nonlinear Phase Noise in Dispersion Unmanaged Fiber-Optic Systems', Saber Rahbarfam and Shiva Kumar

  An analytical expression for the linear and nonlinear phase noise variance in dispersion unmanaged fiber optic systems has been derived using a first-order perturbation theory. Some numerical examples have been provided to illustrate the behavior of the developed phase noise variance in terms of dispersion and distance. The results show that in dispersion unmanaged systems, nonlinear interaction between the amplified spontaneous emission and the signal does not grow as much as in dispersion managed systems, because this interaction is different in each fiber-amplifier span and the noise contributions from various fiber spans do not add up coherently. Therefore, the nonlinear phase variance in a dispersion unmanaged system is much lower than the corresponding noise variance in a dispersion managed system.

- ‘Optimized Physical Carrier Sensing Threshold in High Density CSMA/CA Networks’, Phillip Oni and Steven Blostein

  We address the PCS (physical carrier sensing) threshold selection problem for dense wireless local area networks (WLANs). This important network parameter determines the spatial reuse permitted by the CSMA/CA protocol, which consequently determines the interference level. Using Poisson Point Processes (PPP) from stochastic geometry, we obtain a closed-form expression for PCS threshold selection. Our primary aim is to find the PCS threshold value that improves the spatial density of throughput (SDT). Assuming a Rayleigh fading channel, we derive the PCS threshold as a function of deterministic network parameters (node density and path loss exponent). That is, we determine the optimal PCS threshold based on the fundamental parameters of the network without requiring channel knowledge of each link. To assess the impact of the proposed method, simulation results reveal gains in throughput density over the conventional scheme and the random selection method.

- ‘Extracting the Most Weighted Throughput in UAV Empowered Wireless Systems With Nonlinear Energy Harvester’, Yanjie Dong, Julian Cheng, Md. Jahangir Hossain and Victor C. M. Leung

  With the maturity of unmanned aerial vehicle (UAV) technology, this work investigates the integration of UAV into wireless communication systems. Since the UAV is powered by a capacity-limited battery, this work proposes to use the radio energy harvesting technology at the UAV in order to extend the lifetime of UAV empowered base station. To extract the most weighted throughput of UAV empowered wireless systems, the dirty paper coding scheme and information-theoretic uplink-downlink channel duality are exploited to propose an extracting the most weighted throughput algorithm. Numerical results are used to verify the proposed algorithm.

- ‘Exact Statistical Characterization of RF-Energy Harvesting over Nakagami-m Fading Channel’, Ala Abu Alkheir and Hussein T. Mouftah

  This article gives exact statistical characterization of harvested RF-energy over a Nakagami-m fading channel. In \cite{A.AbuAlkheir1015}, we have shown that the amount of harvested energy is a scaled version of the amount of received energy, which can be statistically modeled using the Sampling Theorem. However, harvesting only happens when the received Signal to Noise Ratio (SNR) exceeds a certain threshold. This article capitalizes on these two results to derive exact closed form expressions of the Cumulative Distribution and Moment Generating Functions (CDF) and (MGF) of the harvested energy over a Nakagami-m fading channel. We also extend the analysis to the case of harvesting over a sequence of N fading blocks. The derived results give researchers a powerful tool to design realistic RF-energy harvesting protocols.

10:20am - 10:40am Coffee Break

10:40 am - 12:00 am (ENG-LG04) Session 3: Coding and Information Theory
Session Chair: Frank Kschischang (UofT)

- 'Reduced Message-Passing bitwidth for Hardware Implementation of ADMM-LP Decoding', Omar Samhan and Stark Draper

  In this paper we consider the implementation in hardware of linear-programming (LP) decoding of low-density parity-check codes. Previous work has shown that the alternating direction method of multipliers (ADMM) can be applied to solve LP decoding in a message passing manner amenable to hardware. Wasson et al.~demonstrated the feasibility of a hardware implementation in a field-programmable gate array (FPGA). However, the area footprint and message bit-width of the implemenation was not competitive with classic alternatives such as min-sum decoding. In this paper we leverage recent work by Jiao et al.~on implementating the central computational primative of ADMM-LP decoding (a certain Euclidean projection) via look-up tables (LUTs). While Jiao's work indicated the possiblity of significant bit-width reduction, it left open a number of questions about how to translate those ideas into hardware and what algorithmic modifications would be required. In this paper we answer those questions and develop a modified version of Wasson's ADMM-LP decoding algorithm, realizing a bit-width reduction of about 50\%, thereby yielding a hardware implementation of ADMM-LP decoding that is competitive with min-sum.

- 'Streaming Codes with Unequal Error Protection against Burst Losses', Mahdi Haghifam, Ahmed Badr, Ashish Khisti, Xiaoqing Zhu, Wai-Tian Dan and John Apostolopoulos

  Error control codes for real-time interactive applications such as audio and video streaming must operate under strict delay constraints and be resilient to burst losses. Previous works have characterized optimal codes that guarantee perfect recovery of all source packets when the burst loss is below a certain maximum threshold. In this work we introduce two notions of unequal error protection (UEP) in streaming codes. The first is symbol-level UEP where each source packet consists of two sub-packets, one of which has higher level of importance than the other. While the important sub-packet has the same deadline it must recover from a longer burst loss. Perfect recovery of the entire source packet is required if the burst loss is below a certain nominal threshold. The second notion is packet-level UEP. Here we assume that the source packets arriving at odd and even times have different levels of importance. When the burst length is below a certain threshold, all the source packets must be recovered. On the other hand, in the period of the longer burst, we only require the recovery of the source packets at even time slots. We discuss practical motivations for both settings and develop coding schemes that use previously proposed streaming codes as constituent codes. We establish optimality or near optimality guarantees through information theoretic converse. Simulation over Gilbert channels show that these codes outperform baseline schemes over a wide range of channel parameters.

- ‘A Direct Method to Construct Golay Complementary Sets Based on Boolean Functions’, Dongxu Ma, Zilong Wang and Guang Gong

  Golay complementary pair and set sequences are highly regarded since their potential in the applications for Peakto-mean power ratio (PMEPR) in multicarrier communications including orthogonal frequency-division multiplexing (OFDM). In the latest literature [13], the authors provided a new construction on Golay complementary sets using matrix method, which also included the Golay complementary pair as a special case. But there is no investigating how these sequences can be efficiently generated. In this paper, we will introduce a method which can directly generate the Boolean functions of q-ary Golay complementary sets with size N and length N^m. From this new method, the generation of the explicit Boolean functions of Golay complementary sets can be used to generate such Golay complementary sets in much more efficient and flexible way. Furthermore, the cost of the implementation of the Golay complementary sets is greatly reduced.

- ‘Subfield Subcodes of Tamo-Barg Locally Recoverable Codes’, Christian Senger and Harsha Kadalveni Shivakumar

  It is shown that Tamo-Barg locally recoverable (LRC) codes can be considered as subcodes of generalized Reed-Solomon (GRS) codes. Their encoding can be interpreted as sequential encoding with two particular constituent codes that depend on each other. The message constraint approach for finding subfield subcodes of GRS codes is transferred to this setting in order to obtain subfield subcodes of LRC codes. The subcodes have the same (or better) locality as their parent codes, and at least their minimum distance.

12:00pm - 1:40pm Lunch

1:40pm - 3:00pm (ENG-LG04) Session 4: Networks and Fog Computing
Session Chair: Chen Feng (UBC)

- ‘A Dynamic Priority Service Provision Scheme for Delay-Sensitive Applications in Fog Computing’, Ali Alnoman and Alagan Anpalagan

  The massive number of connected devices in future networks impose a real challenge in terms of managing both
  communication and computing resources. Moreover, the competency on the limited resources of devices and machines in the IoT era will inherently raise the delay experienced by users. To this end, we propose a dynamic priority service provision scheme to achieve the envisioned ultra-low latency for delay-sensitive applications. First, incoming tasks are classified as delay-sensitive and delay-insensitive, then priority classes are assigned using a matching theory approach where both the task preference and category are taken into account. Secondly, the time delay experienced by each class is investigated on the fog computing node i.e., the edge device, and the communication node i.e., the small base station (SBS), using regular and prioritized queues. To maintain high quality of experience (QoE) in regard with time delay for all tasks, a dynamic priority scheme is proposed and controlled using a heuristic algorithm. The goal of the dynamic priority scheme is to minimize the delay experienced by noncomputing tasks (e.g., regular phone calls) that use the SBS

to obtain radio access links to connect with the cellular network. The combined delay effect of both communication and computing nodes is compared using the different schemes. Results show that the proposed schemes can achieve significant reduction in the amount of delay experienced by users while maintaining the balance between computing and non-computing tasks.

- 'On Base Station Sleeping for Heterogeneous Cloud-Fog Computing Networks', Ali Alnoman and Alagan Anpalagan

  In this paper, a base station sleeping mechanism is investigated taking into account the effect of offloaded tasks on the queue delay at the cloud server. Motivated by the capability of heterogeneous cloud radio access networks (H-CRANs) to efficiently manage and control all network nodes, we aim to minimize power consumption of small base stations (SBSs) under the constraint of queue delay at the central cloud. In the proposed model, computing tasks can be processed either at the edge device close to users, or at the central cloud. The problem is formulated using conditional probabilities whereby the queueing probability of macro base station (MBS) and cloud given that each SBS operates in the sleeping mode is calculated. The sleeping strategy then forces SBSs that impose minimum queueing probability on MBS, cloud, or the union of MBS and cloud to sleep based on the desired performance. The minimum queueing probability on MBS is analogous to the minimum number of tasks approach used in the literature and is used for comparison. Results show that the proposed mechanism can significantly reduce the computing response time in accordance with the desired amount of power saving.

- 'Probabilistic Caching as Mixed Strategies in Spatially-Coupled Edge Caching', Jie Gao, Lian Zhao and Limin Sun

  The problem of probabilistic caching in a network with multiple edge nodes and user nodes is studied. Files with different lengths, caches with different sizes, and spatial coupling through overlapping service areas are considered. The connection between caching probabilities and strategy-mixing probabilities in a mixed strategy is characterized. It is found that a given set of caching probabilities for an edge node can correspond to more than one mixed strategies. Through this characterization, caching probabilities can be decomposed into pure caching strategies and corresponding strategy-mixing probabilities. Moreover, the best-response caching strategy of an EN is studied and obtained based on the spatial-coupling discounted file preference level. The impact of information availability and request scenario on the best-response strategy is analyzed. Numeric examples demonstrate the best-response strategy and the decomposition of the caching probabilities into pure strategies and strategy-mixing probabilities.

- 'Join-the-Idle-Queue Meets the Power-of-*d*-choices', Chunpu Wang, Yonghui Lu, Chen Feng and Julian Cheng

  Power-of-d-choices (Pod) and Join-the-idle-queue (JIQ) are two popular load balancing strategies that have received much attention from both academia and industry. Some possible combinations of Pod and JIQ have been explored very recently. Building upon these works, we have studied two new combinations of Pod and JIQ, which offer several unique advantages such as a better performance-cost tradeoff.

3:00pm - 3:20pm Coffee Break

3:20pm - 5:00pm (ENG-LG04) Session 5: Security
Session Chair: Anas Chaaban (UBC)

- 'Single Packet Authorization in a Multi-layered Security Architecture', Mohammad Mirheydari, Pavol Zavarsky and Sergey Butakov

  Single Packet Authorization (SPA) is a concealment method that hides the open ports, devices, and network components behind a firewall. SPA suffers from a known weakness i.e. the SPA client, and if the SPA client gets compromised by an attacker, the attacker can find his way to the SPA server. This paper explores the possible attacks from the SPA client with the focus on the implementation of SPA in multi-level security architecture such as Industrial Control Systems (ICS). It identifies the limitations of SPA on cascading the authorization packet in multiple security levels and proposes to combine SPA with access control. It is shown in the paper that the security of the whole SPA architecture can be improved by adding some features to the SPA server.

- 'Evaluation of Industrial Firewall Performance Issues in Automation and Control Networks', Davison Zvabva, Pavol Zavarsky, Sergey Butakov and John Luswata

  The IEC 62443 security standards introduce the concepts of zones, conduits, and security levels as a way of segmenting and isolating the sub-systems of an industrial control network. Network segmentation physically/logically partition the control network into separate communication zones to restrict unnecessary flow of traffic between zones of different trust level. Firewalls with deep packet inspection capabilities for filtering industrial control protocols are indispensable elements in implementing important security principles, standards, and best practices of IEC 62443. While partitioning of the industrial control network and placement of multiple firewalls at various locations provides defense in-depth against cyber-attacks, it is important to consider the impact of these firewalls on nodes distributing time critical communications. This paper attempts to (i) study network performance impact introduced by the implementation of multiple firewalls in Modbus TCP/IP industrial control networks following IEC 62443 security standards and (ii) evaluate if time constraint requirements for communications are achievable. The results reveal that the latency and jitters introduced by multilayered firewalls makes it challenging to achieve real-time communications in some industrial applications when strict IEC 62443 security standards are followed.

- 'Analysis of SCADA Security using Penetration Testing: A case study on Modbus TCP Protocol', John Luswata, Pavol Zavarsky, Bobby Swar and Davison Zvabva

  This paper presents an insight into attacks on Supervisory Control and Data Acquisition (SCADA) systems specifically focusing on systems that use the Modbus TCP protocol. A penetration testing approach is adopted using a novel penetration testing tool to (i) test the effectiveness and efficiency of the tool, (ii) examine the insider threat as well as the external threat through internal and external penetration testing respectively and (iii) rate the vulnerabilities identified through the penetration tests according to the Common Vulnerability Scoring System. The study also

examines and tests the existing security countermeasures that are unique to SCADA systems and outlines some recommendations that may improve security in SCADA systems. The experimental results showed that some of the attacks may severely impact integrity and availability.

- 'Secrecy Beamforming for SWIPT MISO Heterogeneous Cellular Networks', Hui Ma, Julian Cheng and Xianfu Wang

In this paper, we consider the secure transmission design for a multiple-input single-output Femtocell overlaid with a Macrocell in co-channel deployment. The Femtocell base station sends confidential messages to information receiving Femtocell users (FUs) and energy signals to energy receiving (ER) FUs while limiting the interference to Macrocell users (MUs). The ER FUs have the potential to wiretap the confidential messages. Consequently, by taking fairness into account, we propose a sum logarithmic secrecy rate maximization beamforming design problem under the interference constraints for MUs and energy harvesting (EH) constraints for ER FUs. The formulated design problem is nontrivial to solve due to the nonconvexity which lies in the objective and the constraints. To tackle with the design problem, a semidefinite relaxation and successive convex approximation based algorithm is proposed. Simulation results demonstrate the effectiveness of the proposed beamforming.