ISITA2006 The 2006 International Symposium on Information Theory and its Applications

COEX, Seoul, Korea
October 29 – November 1, 2006

PROGRAM & ABSTRACTS

Monday 30 October

08.00 Registration

08.30 - 09.30 **PLENARY: Collaboration, Competition and Cognitive Radio Transmission in Wireless Networks, Professor Vahid Tarokh (Harvard University, USA),** GRAND CONFERENCE ROOM (4F)

09.30 - 10.30 **PLENARY: WiBro: A Wireless Broadband Technology, Professor Daehyoung Hong (Sogang University, Korea),** GRAND CONFERENCE ROOM (4F)

10.50 - 11.50 **PLENARY: How to Prove the Security of Cryptography, Dr. Tatsuaki Okamoto (NTT, Japan),** GRAND CONFERENCE ROOM (4F)

11.50 - 14.00 **Lunch**

14.00 - 15.40 **CONCURRENT SESSIONS Mon1-1 - Mon1-5**

	SESSION Mon1-1 **Coding Theory (1)** *Chair: Hitoshi Tokushige (The University of Tokushima)* ROOM: **1**	**SESSION Mon1-2** **Digital Right Management (1)** *Chair: Minoru Kuribayashi (Kobe University)* ROOM: **2**	**SESSION Mon1-3** **Shannon Theory (1)** *Chair: Tomohiko Uyematu (Tokyo Institute of Technology)* ROOM: **3**	**SESSION Mon1-4** **Communication Theory** *Chair: Ikuo Oka (Osaka City University)* ROOM: **4**	**SESSION Mon1-5** **Turbo Codes (1)** *Chair: Hidetoshi Saito (Kogakuin University)* ROOM: **5**
14.00	**A Constraint-Based Design of Short Erasure Codes** *Saejoon Kim, Min-Ho Shin*	**Improvements of the Robustness against Signal Processing by Using Error-Correcting-Codes in Digital Watermarking – Study for Audio Data –** *Satoshi Aoki, Kenji Nagasaka*	**A New Look at Large Deviation Theorems** *Te Sun Han*	**A New Trellis Shaping Design for Peak Power Reduction of Single-Carrier QAM Signals** *Makoto Tanahashi, Hideki Ochiai*	**Performance Evaluation of High-Dimensional Parity Check Code with High Code Rate** *Satoru Kose, Hiroshi Kamabe*
14.20	**Efficient Construction Method of the Best Punctured Convolutional Code** *Yuuki Ogami, Hiroshi Sasano, Takuya Nishimura*	**A Music Watermark in Consideration of MP3 Compression** *Akio Ogihara, Nobuhiko Maeda, Motoi Iwata, Akira Shiozaki*	**Application of Tauberian Theorem to the Exponential Decay of the Tail Probability of a Random Variable** *Kenji Nakagawa*	**A Study on Estimation of Frequency Offset Using EM Algorithm for Multi-Carrier Systems** *Masahiro Fujii, Akihiro Waku, Makoto Itami, Yu Watanabe, Kohji Itoh*	**Study on Turbo Decoding Using Hard Decision Decoder – Principle of Hard-in Soft-out Decoding –** *Kazuhiko Yamaguchi, Shinya Maehara, Brian M. Kurkoski, Kingo Kobayashi*
14.40	**On Construction of Reversible Variable-Length Codes Including Resynchronization Markers as Codewords** *Dongzhao Sun, Hiroyoshi Morita, Mikihiko Nishiara*	**Video Watermark for Detecting Alteration on Spatial Domain and Temporal Domain** *Akio Ogihara, Keisuke Tanaka, Hirofumi Toguchi, Motoi Iwata, Akira Shiozaki*	**Improving and Validating Cramér-Rao Bounds Through Higher-order Asymptotic Estimation Theory: A Case Study** *Justin Dauwels*	**Blind Matched Filter Method for Linear Frequency Modulated Pulse Radar** *Fumio Nishiyama, Hideo Murakami*	**Theoretical Analysis of Bit Error Probability for Convolutional Code with Max-Log MAP Decoding** *Hideki Yoshikawa*
15.00	**A New Class of Binary Constant Weight Codes and Its Decoding Algorithm** *Jun Imai, Yoshinao Shiraki*	**A Scheme of Correlation-based Watermarking for Three-Dimensional Computer Graphics via Topological Data** *Yuuji Kawasaki, Hiromu Koda, Shojiro Sakata*	**Fisher Information and Minimum Test Sample Size** *Choon Peng Tan*	**Detection Scheme for Burst Erasures in Magnetic Recording Channel** *Masayuki Hayashi, Ryuji Kohno*	**Modified EMLMAP Algorithm Using Variable Scaling Factor for Low-power Implemenation of Turbo Decoder** *Jaebum Kim, Jaehong Kim, Byeongjo Kim, Seongsu Park, Hyuncheol Park*
15.20		**A Note on Correlation-based Watermarking Scheme via 1-D SSKF** *Takashi Hayashi, Hiromu Koda, Shojiro Sakata*	**Scaling Property and Tsallis Entropy Uniquely Derived from a Fundamental Nonlinear Differential Equation** *Hiroki Suyari, Tatsuaki Wada*	**A Novel Equalization Algorithm for Frequency-Selective Channels** *Peng Wang, Wee Ser*	

Monday 30 October **continued**

15.40 - 16.00 **Coffee Break**

16.00 - 17.40 **CONCURRENT SESSIONS Mon2-1 - Mon2-5**

	SESSION Mon2-1 **Coding Theory (2)** *Chair: Habong Chung (Hongik University)* ROOM: **1**	**SESSION Mon2-2** **Digital Right Management (2)** *Chair: Motoi Iwata (Osaka Prefecture University)* ROOM: **2**	**SESSION Mon2-3** **Shannon Theory (2)** *Chair: Kenji Nakagawa (Nagaoka University of Technology)* ROOM: **3**	**SESSION Mon2-4** **Communication Systems** *Chair: Martin Schubert (Fraunhofer German-Sino Lab for Mobile Communications)* ROOM: **4**	**SESSION Mon2-5** **Turbo Codes (2)** *Chair: Hideki Yoshikawa (Suzuka National College of Technology)* ROOM: **5**
16.00	**On the Correcting Property of a Two-dimensional Error-correcting Code Based on the Lee Metric on $\mathbb{Z}_{2^m}$** *Banri Bannai, Manabu Hagiwara, Hideki Imai*	**Digital Watermarking with Encrypted Watermarks by Using Masking Effects** *Takahiko Oyachi, Kenji Nagasaka*	**A Class of Average Distributions for Monotone Sources** *Mohammadali Khosravifard, Morteza Esmaeili, Hossein Saidi, T. Aaron Gulliver*	**Modeling of Impulse Noise for Indoor Broadband Power Line Communications** *Daisuke Umehara, Shinji Hirata, Satoshi Denno, Yoshiteru Morihiro*	**Improvements and Extensions of Low-Rate Turbo-Hadamard Codes** *Noriyuki Shimanuki, Brian M. Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi*
16.20	**A Bound on q-ary t-EC-AUED Codes and Constructions of Some Optimal Ternary t-EC-AUED Codes** *Irina Naydenova, Torleiv Kløve*	**Sanitizable Signature Scheme Applying Reversible Data Hiding** *Minoru Kuribayashi, Masakatu Morii*	**Information-Spectrum Characterization of a Multi-terminal Channel with General Correlated Sources** *Ken-ichi Iwata, Yasutada Oohama*	**A Modulation Classification Analysis Using Joint Moments with Linear Transform** *Daisuke Shimbo, Ikuo Oka, Shingo Ata*	**Interleaver Design for a Class of High-Rate Serially Concatenated Codes** *Motohiko Isaka*
16.40	**One Conjecture for Relationship between the Shift Bound and SchaubPlus Bound for Cyclic Codes** *Junru Zheng, Takayasu Kaida*	**Provider Authentication for Bidirectional Broadcasting Service with Fixed Verification Key** *Go Ohtake, Goichiro Hanaoka, Kazuto Ogawa*	**Source Coding of Correlated Gaussian Vector Sources with Several Side Informations at the Decoder** *Yasutada Oohama*	**Intersymbol Interference Compensation Scheme in Collaboration with Transmit Pre-coding and Adaptive Equalization** *Hiroshi Kubo, Shinich Mochida, Katsuyuki Motoyoshi, Takashi Mizuochi, Akihiro Shibuya*	**Stopping Sets for Iterative Row-Column Decoding of Product Codes** *Eirik Rosnes*
17.00		**Specifying the Subtree Number of a Content Distribution Tree Using Visual Cryptography** *Hyunho Kang, Brian M. Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi*	**Multiterminal Source Coding with Complementary Delivery** *Akisato Kimura, Tomohiko Uyematsu*	**Modified PN Code Acquisition Scheme Based on Adaptive Filter Under Frequency Selective Rayleigh Fading Channels** *Donghoon Lee, Kyungwhoon Cheun, Jeongchang Kim*	**The Double Binary Turbo Hybrid ARQ Scheme** *Woo Suk Kwon, Jeong Woo Lee*
17.20		**Subset Incremental Chain Based Broadcast Encryption with Shorter Ciphertext** *Nuttapong Attrapadung, Hideki Imai*			

Tuesday 31 October

08.00 Registration

08.30 - 10.10 **CONCURRENT SESSIONS Tue1-1 - Tue1-5**

	SESSION Tue1-1 **Coding Theory (3)** *Chair: Hiroshi Sasano (Kinki University)*	**SESSION Tue1-2** **Network Security** *Chair: Souhwan Jung (Soongsil University)*	**SESSION Tue1-3** **Source Coding** *Chair: Hiroyoshi Morita (University of Electro-Communications)*	**SESSION Tue1-4** **Spread Spectrum Systems** *Chair: Minoru Okada (Nara Institute of Science and Technology)*	**SESSION Tue1-5** **MIMO (1)** *Chair: Hidekazu Murata (Tokyo Institute of Technology)*
	ROOM: **1**	ROOM: **2**	ROOM: **3**	ROOM: **4**	ROOM: **5**
08.30	**Optimality on Probabilistic Minimax Robust Decoder** *Libo Yang, Lei Wei*	**A New Secret Key Agreement Scheme Based on Eigenvalues of Channel Matrices in Phase-Controlled MIMO Systems** *Kengo Hiwatashi, Hideki Ochiai, Junji Shikata*	**Universal Lossy Coding for Individual Sequences Based on Complexity Functions** *Shigeaki Kuzuoka, Tomohiko Uyematsu*	**Impact of Narrowband Interference for DS-multiband-UWB Wireless Communications** *Yun-Seok Song, Shigenobu Sasaki, Chin Sean Sum, Hisakazu Kikuchi*	**Communication over Hypercomplex Kähler Manifolds: Capacity of Dual-Polarized Multidimensional-MIMO Channels** *Özgür Ertuğ*
08.50	**A Comparison between WB Algorithm and BM Algorithm** *Shojiro Sakata, Masaya Fujisawa*	**A Study on Detection of Varied Worms with Analyzing Session Information** *Il-Ahn Cheong, Taek-Yong Nam*	**On the Optimum Performance Theoretically Attainable for Scalarly Quantized Correlated Sources** *Thorsten Clevorn, Laurent Schmalen, Peter Vary, Marc Adrat*	**On Interference Mitigation of DS-Multiband-UWB System Over Indoor Multipath Environment** *Chin Sean Sum, Shigenobu Sasaki, Hisakazu Kikuchi*	**Transceiver Optimization for Multiuser MIMO Systems: Min-Max Relative User-MSE under a Total Power Constraint** *Shuying Shi, Martin Schubert, Holger Boche*
09.10	**On Behavior of RS-decoder Based on Welch-Berlekamp Algorithm for $t+\mu$ Errors** *Masami Mohri, Masakatu Morii*	**Reliability Improved Port Knocking Scheme** *Hiroyuki Tanaka, Takashi Katoh, Bhed Bahadur Bista, Toyoo Takata*	**Bounds on Exponentiated Expected Length of Optimal Binary Prefix Codes** *Yen-Yi Lee, Jay Cheng*	**Short and Efficient Frequency Hopping Sequences** *Young-Joon Kim, Dae-Son Kim, Hong-Yeop Song*	**Selecting a Near-Optimal Set of Joint Transmit-Receive Antennas for a MIMO Channel Based on Maximizing Channel Capacity** *Hyo-Shil Kim, Sung-Yeon Kim, Youn-Shik Byun*
09.30	**An Improvement to an Iterative Bounded-distance and Encoding-based Decoding Algorithm for Binary Linear Block Codes** *Hitoshi Tokushige, Marc Fossorier, Toru Fujiwara, Tadao Kasami*	**An IP Traceback Scheme with Variably Probabilistic Packet Marking** *Takeaki Terada, Masakazu Soshi, Atsuko Miyaji*	**Improving LZ77 Data Compression Using Bit Recycling** *Danny Dube, Vincent Beaudoin*	**Throughput Performance of the MPPM DS/SS ALOHA System on the AWGN Channel** *Masayuki Matsuzaki, Fumie Ono, Hiromasa Habuchi*	**On the Complexity of Feedback Generation in MISO Beamforming and Diversity Schemes** *Albrecht J. Fehske, Patrick Marsch, Gerhard P. Fettweis*
09.50	**Method for Generating a Competing Codeword Using a Chain of Minimum Distance Searches** *Jun Asatani, Takuya Koumoto, Toru Fujiwara, Tadao Kasami*	**Implementation and Evaluation of Dynamic Process Resolution Protocol Actualizing Location Transparency** *Hidekazu Suzuki, Akira Watanabe*	**Linear-Time Encodable and Decodable Codes for Slepian-Wolf Source Networks** *Tomohiko Uyematsu*	**Construction of Continuous-Time Equivalents of Welch Bound Equality Sequences** *Joon Ho Cho*	

10.10 - 10.30 **Coffee Break**

Tuesday 31 October continued

10.30 - 12.10 **CONCURRENT SESSIONS Tue2-1 - Tue2-5**

	SESSION Tue2-1 **LDPC Codes (1)** *Chair: Sae-Young Chung (KAIST)* ROOM: **1**	**SESSION Tue2-2** **Data Security** *Chair: Shunsuke Araki (Kyushu Institute of Technology)* ROOM: **2**	**SESSION Tue2-3** **Shannon Theory (3)** *Chair: Yasutada Oohama (Kyushu University)* ROOM: **3**	**SESSION Tue2-4** **UWB** *Chair: Shigenobu Sasaki (Nigata University)* ROOM: **4**	**SESSION Tue2-5** **MIMO (2)** *Chair: Eiji Okamoto (Nagoya Institute of Technology)* ROOM: **5**
10.30	**A Minimum Weight Test for a Certain Subclass of Array LDPC Codes** *Kenji Sugiyama, Yuichi Kaji*	**Perfect $(2, n)$ Threshold Secret Sharing Systems Based on Binary Matrices with Constant Column Weight** *Todorka Alexandrova, Hiroyoshi Morita*	**Channel Coding Theorem for Discrete Multipath Channel** *Yoichiro Watanabe, Koichi Kamoi*	**Effect of Multi-path on Rake Reception for UWB-IR Communications** *Isamu Matsunami, Keiji Terasaka, Kenji Higashikatsuragi, Akihiro Kajiwara*	**Influence of Transmit and Receive Correlations on Performance of the MIMO System with Multiple Antennas and Relay Terminals** *Ryosuke Uchida, Hiraku Okada, Takaya Yamazato, Masaaki Katayama*
10.50	**On Minimal Length of Quasi Cyclic LDPC Codes with Girth ≥ 6** *Manabu Hagiwara, Koji Nuida, Takashi Kitagawa, Marc Fossorier, Hideki Imai*	**Collision-Controllable Hash Function** *Hidenori Kuwakado, Masakatu Morii*	**Outage Behavior of Discrete Memoryless Channels Under Channel Estimation Errors** *Pablo Piantanida, Gerald Matz, Pierre Duhamel*	**Experimental Evaluation of In-home UWB-IR Propagation Characteristics** *Keiji Terasaka, Kenji Higashikatsuragi, Isamu Matsunami, Akihiro Kajiwara*	**On Iterative Decoding in Multiuser Space-Time Coding Systems** *Ha H. Nguyen, Yajun Yang, Ed Shwedyk*
11.10	**Use of Dynamic Programming for the Design of Irregular LDPC Codes** *Sang Hyun Lee, Duho Rhee, Il Mu Byun, Kwang Soon Kim*	**A Cache Attack on SEED** *Yoshitaka Ikeda, Takenori Ichikawa, Toshinobu Kaneko*	**Improved Bounds for the Capacity of the Binary Deletion Channel** *Hugues Mercier, Vijay K. Bhargava*	**Optimality of Modulated Hermite Pulses for UWB/PPM Systems** *Burak Berksoy, Lei Wei*	**Sphere Decoder for Imperfect Channel State Estimation** *Chimato Koike, Ryutaroh Matsumoto, Tomohiko Uyematsu*
11.30	**New Bit Mapping Scheme of Irregular LDPC Codes for Nonuniform Gaussian Channels** *Hyeong-Gun Joo, Song-Nam Hong, Dong-Joon Shin*	**A Categorizing-Guessed-Values Approach for the Key Recovery Attack against WEP** *Toshihiro Ohigashi, Yoshiaki Shiraishi, Masakatu Morii*		**Multi-Band Ultra-Wide Bandwidth Data Transmission Using Raised Cosine Pulse Shaping** *Chaiyaporn Khemapatapan*	**Multirate Multiuser Code for Multiple-Access Adder Channel** *Jun Cheng, Koichi Kamoi, Yoichiro Watanabe*
11.50		**A Method for Checking the Parity of $(\#J_C - 1)/2$** *Masataka Akane, Yasuyuki Nogami, Yoshitaka Morikawa*		**A Simple Non-Coherent Detector for OOK on UWB Channels** *Burak Berksoy, Lei Wei*	

12.10 - 14.00 **Lunch**

Tuesday 31 October continued

14.00 - 15.40 **CONCURRENT SESSIONS Tue3-1 - Tue3-5**

	SESSION Tue3-1 **LDPC Codes (2)** *Chair: Lei Wei (University of Central Florida)* ROOM: **1**	**SESSION Tue3-2** **Public Key Cryptography** *Chair: Dong-Joon Shin (Hanyang University)* ROOM: **2**	**SESSION Tue3-3** **Multi-User Information Theory** *Chair: Yoichiro Watanabe (Doshisha University)* ROOM: **3**	**SESSION Tue3-4** **CDMA** *Chair: Shinji Tsuzuki (Ehime University)* ROOM: **4**	**SESSION Tue3-5** **MIMO (3)** *Chair: Kiyomichi Araki (Tokyo Institute of Technology)* ROOM: **5**
14.00	**Complete Erasure Recovery of Irregular Repeat-accumulate Codes** *Saejoon Kim*	**Efficient Multiple Encryption from OW-PCA Primitives** *Yang Cui, Kazukuni Kobara, Hideki Imai*	**Optimal Resource Allocation for a Bidirectional Regenerative Half-duplex Relaying** *Tobias J. Oechtering, Holger Boche*	**A Non-Gaussian Coding Scheme that Exceeds Conjectured Gaussian Capacity Limit in CDMA Transmission with Single-User Decoding** *Aminata Amadou Garba, Jan Bajcsy*	**A Practical Vector Dirty Paper Coding Scheme for MIMO Gaussian Broadcast Channels** *Shih-Chun Lin, Hsuan-Jung Su*
14.20	**Cycle Analysis and Interleaver Design of Finite-Length Punctured LDPC Codes with Dual-Diagonal Parity Structure** *Yong Chun Piao, Dong-Joon Shin*	**A Simple Approach to Evaluate Fujisaki-Okamoto Conversion in Identity Based Encryption** *Peng Yang, Takashi Kitagawa, Goichiro Hanaoka, Rui Zhang, Hajime Watanabe, Kanta Matsuura, Hideki Imai*	**Characterization of Optimal Resource Assignments in the Framework of Blocking System Theory** *Marcin Wiczanowski, Holger Boche, Slawomir Stanczak*	**CDMA Signal Design to Optimize Trade-off between the Bandwidth-efficiency and Power-efficiency in Uplink Systems** *Atsurou Handa, Masahiro Fujii, Makoto Itami, Kohji Itoh*	**Approximate MLD for MIMO Systems Using Error Detection Scheme Based on LRAD** *Dong-Jin Lee, Ryun-Woo Kim, Youn-Shik Byun*
14.40	**Analysis of Generalized LDPC Codes with Random Component Codes for the Binary Erasure Channel** *Enrico Paolini, Marc Fossorier, Marco Chiani*	**Notes on Several ID Based Cryptosystems** *Ryuichi Sakai*	**Characterization of the Fairness Gap in Resource Allocation for Wireless Cellular Networks** *Holger Boche, Marcin Wiczanowski, Slawomir Stanczak*	**Localization of Radio-Controlled Car by Acoustic DS-CDM Signals** *Shinji Tsuzuki, Naoyuki Takeichi, Yutaka Tano, Yoshio Yamada*	**Code Controlled Sphere Decoding of Four Efficient MISO Lattices** *Camilla Hollanti*
15.00	**Performance of Low-Density Parity-Check Codes for Burst Erasure Channels** *Gou Hosoya, Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa*	**A Public-Key Identification Scheme Based on a New Lattice Problem** *Shunichi Hayashi, Mitsuru Tada*	**On the Transport Capacity of Wireless Ad-hoc Networks** *Sae-Young Chung*	**Generalized Random Spreading Performance Analysis of CDMA over GWSSUS Fading Channels** *Özgür Ertuğ*	**A Consideration on the Complexity Reduction of LDPC Coded MIMO OFDM Receiver Structure** *Le Khoa Nguyen, Yasunori Iwanami, Eiji Okamoto*
15.20	**Concatenated Coding System with Array and LDPC Codes for Burst-Error Channel** *Hidetoshi Saito, Masayuki Hayashi, Ryuji Kohno*	**An Efficient N-Party Password-based Authenticated Key Exchange Protocol** *SeongHan Shin, Kazukuni Kobara, Hideki Imai*	**An Algebra for Log-Convex Interference Functions** *Holger Boche, Martin Schubert, Marcin Wiczanowski*	**Generalized MPSC and Its Performance in Synchronous Optical CDMA Systems** *Tomoko K. Matsushima, Yasuaki Teramachi*	

15.40 - 16.00 **Coffee Break**

Tuesday 31 October **continued**

16.00 - 17.40 **CONCURRENT SESSIONS Tue4-1 - Tue4-5**

	SESSION Tue4-1	**SESSION Tue4-2**	**SESSION Tue4-3**	**SESSION Tue4-4**	**SESSION Tue4-5**
	Iterative Decoding	**Data Network**	**Network Coding**	**Mobile Communications**	**OFDM**
	Chair: Kenta Kasai (Tokyo Institute of Technology)	*Chair: Yoshiaki Shiraishi (Nagoya Institute of Technology)*	*Chair: Ken-ichi Iwata (Yamagata University)*	*Chair: Kyungwhoon Cheun (POSTECH)*	*Chair: Makoto Itami (Tokyo University of Science)*
	ROOM: **1**	ROOM: **2**	ROOM: **3**	ROOM: **4**	ROOM: **5**
16.00	**Reducing Computational Cost on Modified MDBF Decoding for High Dimensional Parity-Check Code** *Yuuki Funahashi, Shogo Usami, Akira Ogawa, Ichi Takumi, Masayasu Hata*	**Researches on Mobile Communications over a Private Address Area and a Global Address Area** *Kazuto Enomoto, Hidekazu Suzuki, Junichi Sakamoto, Akira Watanabe*	**Characterization of Communication Cost Using an Information Theoretic Approach** *Terence H. Chan*	**A Consideration for Protection Ratio of Radio Relay System with Diversity Techniques for Frequency Coordination** *Kyoung-Whoan Suh, Joohwan Lee*	**New Selection Method of Near Optimal PRT Set in TR Scheme for PAPR Reduction of OFDM** *Dae-Woon Lim, Hyung-Suk Noh, Jong-Seon No, Dong-Joon Shin*
16.20	**Reduced-Complexity Decoding of LDPC Codes Based on the Sum-Product Algorithm** *Seho Myung, Kyeongcheol Yang*	**A Proposal of Voice over IP Passing through Firewall and Its Evaluation** *Masashi Ito, Akira Watanabe*	**Architecture for Efficiently Decodable Network Codes** *Terence H. Chan*	**An Improvement of Closed-loop Transmit Diversity with Three Transmit Antennas** *Manabu Sugawara, Eiji Okamoto, Yasunori Iwanami*	**Frequency Domain Turbo Equalization Combined with Frequency Offset Compensation in Uplink OFDMA Systems** *Yuusuke Miyauchi, Takahiko Saba*
16.40	**On the Implementation of Belief Propagation (BP) Algorithm for Decoding Low-Density Parity-Check (LDPC) Codes** *Young Seob Lee, Min Seok Oh, Jin Sung Choi*	**Researches on Connections between WAPL and the Internet** *Yoshiyuki Kato, Masashi Ito, Akira Watanabe*	**Calculus of Service Guarantees for Network Coding** *Ali Mahmino, Jérôme Lacan, Christian Fraboul*	**A Study on Route Diversity Effect Using Turbo Codes in Mesh Networks** *Tadahiro Wada, Abbas Jamalipour*	**Turbo Detector Using Modified SISO-MLD for CCI Suppression in LDPC Coded SDM-OFDM Systems** *Shoichi Sasahara, Takahiko Saba*
17.00	**On the Decoding of LDPC Codes in IEEE 802.16e Standards for Improving the Convergence Speed** *Min-Ho Jang, Beomkyu Shin, Woo-Myoung Park, Jong-Seon No, In San Jeon*	**Using Hybrid Method to Detect Internet Worms by Analyzing ICMP Type 3 Messages and Worm Characteristic Matching** *WenHung Su, JaeHo Lee, Tomokazu Nagata, Shiro Tamaki*		**Analysis of Jong Nang Multiple Access Channel** *MoonHo Lee, Xuegin Jiang, Chang-hui Choe, Sung Hoon Kim*	**Reactance-domain Modulation Scheme for Burst Error Reduction of ISDB-T in Slow Fading Environment** *Young-Cheol Yu, Minoru Okada, Heiichi Yamamoto*
17.20	**Analysis of Complexity and Convergence Speed of Sequential Schedules for Decoding LDPC Codes** *Sunghwan Kim, Min-Ho Jang, Jong-Seon No, Song-Nam Hong, Dong-Joon Shin*	**An Error Control Scheme for the Routing Control Onboard the Satellite Repeater** *Shunsuke Saiki, Akira Ogawa, Takaya Yamazato*		**A Simple Cooperative Mobile Selection in Cooperative Diversity System** *Sung-Yeon Kim, Hyo-Shil Kim, Youn-Shik Byun*	**Delay and Buffer Size Bounds for OFDM Broadcast Systems** *Gerhard Wunder, Chan Zhou, Thomas Michel*

18.00 - **Banquet, JANBOGO HALL (3F, 335+336)**

Wednesday 1 November

08.00 Registration

08.30 - 10.10 **CONCURRENT SESSIONS Wed1-1 - Wed1-5**

	SESSION Wed1-1	**SESSION Wed1-2**	**SESSION Wed1-3**	**SESSION Wed1-4**	**SESSION Wed1-5**
	Weight Distribution	**Quantum Information Processing (1)**	**Random Number**	**Sensor Networks**	**Image & Speech**
	Chair: Marc Fossorier (University of Hawaii)	*Chair: Koichi Yamazaki (Tamagawa University)*	*Chair: Hidenori Kuwakado (Kobe University)*	*Chair: Justin Dauwels (Riken Brain Science Institute)*	*Chair: Hiroshi Kamabe (Gifu University)*
	ROOM: **1**	ROOM: **2**	ROOM: **3**	ROOM: **4**	ROOM: **5**
08.30	**Asymptotic Average Coset Weight Distribution of Multi-Edge Type LDPC Code Ensembles** *Kenta Kasai, Yuji Shimoyama, Tomoharu Shibuya, Kohichi Sakaniwa*	**Property of Optimum Quantum Detection for Mixed States with Non Gaussian and Gaussian Noise** *Toshiyuki Tsuchimoto, Tomohiro Sawada, Shogo Usami, Tsuyoshi Sasaki Usuda, Ichi Takumi*	**Generation of a Discrete Distribution Using Biased Coins** *Danielle P. B. de A. Camara, Valdemar C. da Rocha Jr., Cecilio Pimentel*	**Measurement of Distance Between Nodes in an Ad-hoc Network by Multiple Acoustic Waves** *Wataru Uemura, Masashi Murata*	**Sign-only Synthesis** *Zhimei Yang, Hiroshi Kondo, Takaharu Koda, Lifeng Zhang*
08.50	**Support Weight Distribution of Regular LDPC Code Ensembles** *Takayuki Itsui, Kenta Kasai, Ryoji Ikegaya, Tomoharu Shibuya, Kohichi Sakaniwa*	**Characteristics of Classical Capacity of an Attenuated Channel Assisted by Orthogonal Entangled States** *Seiji Hattori, Tsuyoshi Sasaki Usuda*	**Analysis for Pseudorandom Number Generators Using Logistic Map** *Shunsuke Araki, Takeru Miyazaki, Satoshi Uehara*	**Acoustic Sensing for Detection of Approaching Vehicles** *Kensaku Asahi, Fumiyasu Miyoshi, Akira Ogawa*	**Statistical Methods for a Large Vocabulary Continuous Speech Recognition System for Hindi** *Kshitij Gupta, Pramod Kumar Sharma*
09.10	**New Probabilistic Algorithm to Enhance the Reliability of Computed Weight Distribution of LDPC Codes** *Masanori Hirotomo, Masami Mohri, Masakatu Morii*	**Counter-examples of the Trace Inequalities Related to the Auxiliary Function of the Quantum Reliability Function** *Shigeru Furuichi, Kenjiro Yanagi*	**Correction of Overlapping Template Matching Test Included in NIST Randomness Test Suite** *Kenji Hamano, Toshinobu Kaneko*	**Bayes Stopping Rule for Wireless Sensor Networks** *Jin Kyung Park, Woo Cheol Shin, Jun Ha, Cheon Won Choi*	**Supplement to a Theorem for Biorthogonal Bases of Wavelets and a Consideration of Four-term Sequence** (h_n) *Hajime Sato*
09.30	**An Efficient Method for Computing the Minimum Weight of High Rate Binary Cyclic Codes** *Zheyu Li, Masami Mohri, Masakatu Morii*	**Artificial but Fully Quantum Description Approach to Quantum State Distinction Problem** *Kentaro Imafuku, Hideki Imai*	**A Keystream Resynchronization by Time and Precision Information** *Janghong Yoon*	**Iterative Joint Channel-Decoding Scheme Using the Correlation of Transmitted Information Sequences in Sensor Networks** *Kentaro Kobayashi, Takaya Yamazato, Hiraku Okada, Masaaki Katayama*	**Application of Background Subtraction with Renewable Background to Gesture Region Extraction** *Akio Ogihara, Hiroshi Matsumoto, Akira Shiozaki*
09.50	**On Relation between the Defining Set and the Weight Distribution for Cyclic Codes** *Takayasu Kaida, Junru Zheng*		**An Effective Simple Fuzzy Approach for Stable Real Random Number Generator** *Sunchun Park, Youngmi Park, Daesun Park, Chunsu Kim, ChoogHo Cho*		**A Study on the Expansion of a Resolution Conversion Method into Rational Scale Using Neighboring Blocks' DCT Coefficients** *Tomio Goto, Yoshihiro Shinkai, Masaru Sakurai, Tadashi Kitamura*

Wednesday 1 November continued

10.10 - 10.30 **Coffee Break**

10.30 - 11.50 **CONCURRENT SESSIONS** **Wed2-1 - Wed2-5**

	SESSION Wed2-1	**SESSION Wed2-2**	**SESSION Wed2-3**	**SESSION Wed2-4**	**SESSION Wed2-5**
	Coded Modulation and Space-Time Codes *Chair: Kazuhiko Yamaguchi (University of Electro-Communications)*	**Quantum Information Processing (2)** *Chair: Ryutaroh Matsumoto (Tokyo Institute of Technology)*	**Pattern Recognition** *Chair: Tomoko K. Matsushima (Polytechnic University)*	**Ad Hoc Networks** *Chair: Takaya Yamazato (Nagoya University)*	**Sequences** *Chair: Takayasu Kaida (Kinki University)*
	ROOM: **1**	ROOM: **2**	ROOM: **3**	ROOM: **4**	ROOM: **5**
10.30	**Improved Decoding for Trellis Coded Modulation with a Convolutional Processor** *Yeong-Luh Ueng, Ruey-Yi Wei, Chia-Jung Yeh, Mao-Chao Lin, Jun-Yun Lu*	**Entanglement of Formation of a Decohered Quasi-Bell State** *Ryutaro Yamamoto, Tsuyoshi Sasaki Usuda, Ichi Takumi*	**A Note on Spelling Correction Methods Based upon Statistical Decision Theory** *Yasunari Maeda, Hideki Yoshida, Yoshitaka Fujiwara, Toshiyasu Matsushima*	**Equalization Techniques for Multihop Cooperative Wireless Networks with Asynchronous Relaying** *Ryu Yamashita, Hidekazu Murata, Susumu Yoshida, Kiyomichi Araki*	**Correlation Distribution of Quadriphase ZCZ Sequences Obtained from a Perfect Sequence and a Unitary Matrix** *Shuichi Jono, Satoshi Uehara*
10.50	**Golden Space-Time Trellis Coded Modulation** *Yi Hong, Emanuele Viterbo, Jean-Claude Belfiore*	**Quantum Secure Direct Communication Protocols for Sending a Quantum State** *Yumiko Murakami, Masaki Nakanishi, Manabu Hagiwara, Shigeru Yamashita, Yasuhiko Nakashima*	**Fast Nearest Neighbor Search Algorithm for Waveform Quantization Using Reflection Group** *Shuichi Maki, Nobumoto Yamane, Yoshitaka Morikawa*	**Adaptive Modulation Schemes for Multihop Cooperative Wireless Networks** *Bao Thi Ngoc Pham, Hidekazu Murata, Susumu Yoshida, Kiyomichi Araki*	**Higher Dimensional Complete-Complementary Sequences: A General Approach** *R. S. Raja Durai, Naoki Suehiro*
11.10	**New Optimal Rate-Diversity Tradeoff Space-Time Codes with Adaptive Iterative Decoding** *Wen-Hsien Chiu, Hsuan-Jung Su*	**Uncertainty Principle and Oblivious Transfer** *Takayuki Miyadera, Hideki Imai*	**The Entropy Potential of a Discrete Probability Distribution** *Jan Poland*	**Adaptive Node Selection Algorithm for Co-operative Multi-hop Networks** *Ryu Atsuta, Takahiko Saba*	**On the Relationship of Sidel'nikov Sequences** *Tae-Hyung Lim, Young-Sik Kim, Jung-Soo Chung, Jong-Seon No*
11.30	**Performance Comparison Between Conventional Space-Time Block Code and Proposed Constellation Rotation Space-Time Codes** *Mea-Hwa Park, Hyo-Shil Kim, Jong-Deuk Kim, Youn-Shik Byun*	**Perfect Single-Error-Correcting Binary Code for Interactive Secret Key Reconciliation** *Koichi Yamazaki*	**User Verification Method by Biometric Feature in Keystroke Motion and Key Press Timing** *Akio Ogihara, Hiroyuki Matsumura, Akira Shiozaki*	**Implementation of Mobile PPC Realizing Mobility of Mobile Nodes** *Masaki Sejimo, Akira Watanabe*	

ISITA2006 The 2006 International Symposium on Information Theory and its Applications

COEX, Seoul, Korea
October 29 – November 1, 2006

ABSTRACTS

Mon1-1 : Coding Theory (1)

A Constraint-Based Design of Short Erasure Codes

Saejoon Kim, Min-Ho Shin

The design of erasure codes of short code lengths is considered. The proposed codes perform pretty well and significantly outperform optimal degree distribution-generated codes. It is also shown that the use of regular codes suffices to achieve very low loss recovery failure probability and that LDPC codes are inherently superior to the extended IRA codes of Yang et al. at finite code lengths.

Efficient Construction Method of the Best Punctured Convolutional Code

Yuuki Ogami, Hiroshi Sasano, Takuya Nishimura

It has been shown that for any punctured convolutional code there exists a high rate convolutional code (equivalent code) whose weight spectrum is the same as that of the punctured code. We present a new method for constructing best punctured convolutional codes. In the method, we search for the best equivalent code and derive the best punctured code from it. Using the method, we can reduce the number of candidates of the high rate code then we can obtain best punctured codes with relatively large constraint length. We show some new best punctured convolutional codes with rates $R = (n-1)/n, (n = 1, 2, \cdots, 10)$.

On Construction of Reversible Variable-Length Codes Including Resynchronization Markers as Codewords

Dongzhao Sun, Hiroyoshi Morita, Mikihiko Nishiara

A reversible variable-length code (RVLC) is a code such that no codeword is a prefix or a suffix of any other codeword. An RVLC can decode backward as well as forward starting at a special resynchronization marker (re-sync) that is periodically inserted into the sequence of codewords. In this paper, we propose an algorithm to construct an RVLC in which some codewords function as re-sync. Some codewords in the RVLC are replaced by minimum forbidden words (MFW) of a sequence of codewords. MFWs can be obtained from the antidictionary associated with the sequence.

A New Class of Binary Constant Weight Codes and Its Decoding Algorithm

Jun Imai, Yoshinao Shiraki

This paper proposes a new class of binary constant weight codes as well as a decoding algorithm for it. Let $A(n, d, w)$ denote the maximum possible number of code words in binary (n, d, w) constant weight codes. Unknown instances still remain for larger (n, d, w)s. The proposed class of binary constant weight codes fills in the remaining blank instances of (n, d, w)s . Our new construction technique is performed by considering a triad $(G, \Omega, f) :=$ ("Group G", "Set Ω, "Action f on Ω") simultaneously. Moreover, we describe a decoding algorithm for proposed class of constant weight codes.

Mon1-2 : Digital Right Management (1)

Improvements of the Robustness against Signal Processing by Using Error-Correcting-Codes in Digital Watermarking – Study for Audio Data –

Satoshi Aoki, Kenji Nagasaka

This note is an improvement of our former notes [5], [1] and [2]. For [5], we do not have physical random number generating device, but the frame work of digital watermarking for audio signal data is settled. The physical random number generating device made by Aoki[1] has outputs with so small value of autocorrelation function that we consider this property to apply spectrum spreading. Indeed this idea is affirmative in [2]. Then to tackle the difficult problem of breaking digitalwatermarking embedded, introduce error correcting code and against the detection trial introduce an encryption system. Those two introduction is our idea and for the moment, our idea may not give enough results and remains many problems.

A Music Watermark in Consideration of MP3 Compression

Akio Ogihara, Nobuhiko Maeda, Motoi Iwata, Akira Shiozaki

Recently, copyright infringement becomes a social problem such as some rogues illegally distribute the reproduction on the Internet. These illegal distributors often use MP3 (MPEG audio layer-3) compression which is usually used in personal computer, portable IC audio player, etc. MP3 compression occasionally erases the digital watermark which is prevention technique against the copyright infringement. Hence we propose a new watermarking method for audio data in consideration of MP3 compression. In the proposed method, watermark is embedded in large MDCT (modified discrete cosine transform) coefficients by avoiding small MDCT coefficients, because it is highly possible that the magnitude relation of small MDCT coefficients is destroyed by MP3 compression. Moreover, we improve the above method by avoiding the fragile large MDCT coefficients according to the correlation between the fragileness of MDCT coefficients and the parameters which are used in MP3 encoding process.

Video Watermark for Detecting Alteration on Spatial Domain and Temporal Domain

Akio Ogihara, Keisuke Tanaka, Hirofumi Toguchi, Motoi Iwata, Akira Shiozaki

We propose a new video watermarking method for detecting alteration. In the proposed method, the watermark for each frame (frame length = 1/30 second) is determined by a secret key, and then it is embedded in LL4 DWT (discrete wavelet transform) coefficient of image data and MDCT (modified discrete cosine transform) coefficient of sound data. By checking whether extracted watermark is correct or not, we can detect the alteration of the video data. By using the proposed method, we can detect alteration on both spatial domain and temporal domain.

A Scheme of Correlation-based Watermarking for Three-Dimensional Computer Graphics via Topological Data

Yuuji Kawasaki, Hiromu Koda, Shojiro Sakata

In this paper we propose a scheme of correlation-based watermarking for three-dimensional(3-D) computer graphics via topological data, and examine the resistance to some fundamental attacks. First, we formulate the structure of 3-D polygonal models. Next, we explain a spread sequence(i.e. M-sequence) that is concerned with our scheme, and propose a scheme of correlation-based watermarking for 3-D computer graphics via topological data. The experimental results for some test models show that the watermark information in each model can be detected by our scheme even when the watermarked models are subjected to attack such as additive random noise.

A Note on Correlation-based Watermarking Scheme via 1-D SSKF

Takashi Hayashi, Hiromu Koda, Shojiro Sakata

In this paper, we present a scheme of correlation-based watermarking via 1-D SSKF(Symmetric Short Kernel Filter). First, we formulate 5/3 taps SSKF, orthogonal transform and biorthogonal transform. Next, we explain an oblivious algorithm for the watermarking in wavelet transform (WT) domain, which need not refer to original images in order to detect watermarks. The experimental results for some test images show that watermark information in each image can be detected sensitively by our scheme even when the watermarked images are subjected to processing technique such as clipping.

Mon1-3 : Shannon Theory (1)

A New Look at Large Deviation Theorems

Te Sun Han

In this paper we show some new look at large deviation theorems from the viewpoint of the informationspectrum (IS) methods, which has been first exploited in information theory, and also demonstrate a new basic formula for the large deviation rate function in general, which is expressed as a pair of the lower and upper IS rate functions.

Application of Tauberian Theorem to the Exponential Decay of the Tail Probability of a Random Variable

Kenji Nakagawa

We give a sufficient condition for the exponential decay of the tail probability of a non-negative random variable. We consider the Laplace-Stieltjes transform of the probability distribution function of the random variable. We show a theorem that if the abscissa of convergence of the LS transform is negative finite and the real point on the axis of convergence is a pole of the LS transform, then the tail probability decays exponentially. For the proof of the theorem, we extend and apply so-called a finite form of Ikehara's complex Tauberian theorem by Graham-Vaaler.

Improving and Validating Cramér-Rao Bounds Through Higher-order Asymptotic Estimation Theory: A Case Study

Justin Dauwels

The Cramér-Rao bound (CRB) is a well-known lower bound on the mean square estimation error. The CRB has been computed for numerous estimation problems in digital communications, signal processing, and beyond. In many interesting applications (as for example phase, frequency and timing synchronization, which are estimation problems that appear in the context of digital communications), the Cramér-Rao bound is only valid in the limit of an infinite number of observations. In practice, the number of observations is obviously finite and the CRB may not be applicable. For example, the CRB for the problem of phase estimation (with a finite number of observations) is invalid for low signal-to-noise ratios. In this paper, we demonstrate (by means of higher-order asymptotic estimation theory) (i) how the validity of the CRB (for a finite number of observations) can be verified; (ii) how the CRB can be improved. As an illustration, we consider the problem of joint phase and variance estimation.

Fisher Information and Minimum Test Sample Size

Choon Peng Tan

It is well-known that the maximum likelihood estimator of a parameter has an asymptotic normal distribution subject to certain regularity conditions. We consider a simple hypotheses testing problem where a normalized maximum likelihood estimator is used as a test statistic. The Fisher index of discrimination of this test statistic is shown to be a function of the sample size and the Fisher informations of the probability density functions under testing. Utilizing a previous theorem of the author, we show that the Fisher index converges to a constant depending only on the pre-assigned Type I and Type II error probabilities as the minimum sample size required for the test goes to infinity. This result can be applied to estimate the minimum sample sizes of tests using the Fisher informations. In particular, we consider tests on certain functions of the parameters of a probability density function belonging to the regular exponential class using a normalized version of a maximum likelihood estimator achieving the Cramér-Rao lower bound for the variance of the unbiased estimators of that function of the parameter. In this case, there is a clear relationship between the Fisher information and the minimum test sample size in the limit of the Fisher index.

Scaling Property and Tsallis Entropy Uniquely Derived from a Fundamental Nonlinear Differential Equation

Hiroki Suyari, Tatsuaki Wada

We derive a scaling property from a fundamental nonlinear differential equation whose solution is the so-called q-exponential function. A scaling property has been believed to be given by a power function only, but actually more general expression for the scaling property is found to be a solution of the above fundamental nonlinear differential equation. In fact, any power function is obtained by restricting the domain of the q -exponential function appropriately. As similarly as the correspondence between the exponential function and Shannon entropy, an appropriate generalization of Shannon entropy is expected for the scaling property. Although the q-exponential function is often appeared in the optimal distributions of some one-parameter generalized entropies such as Rényi entropy, only Tsallis entropy is uniquely derived from the algebra of the q -exponential function, whose uniqueness is shown in the two ways in this paper.

Mon1-4 : Communication Theory

A New Trellis Shaping Design for Peak Power Reduction of Single-Carrier QAM Signals

Makoto Tanahashi, Hideki Ochiai

In this paper, we propose a new trellis shaping design for peak power reduction of single-carrier QAM signals. Simulation results show that significant reduction of peak power can be achieved. The performance of the proposed system is also compared with several other known peak power reduction techniques in terms of the trade-offs between peak power efficiency and information rate.

A Study on Estimation of Frequency Offset Using EM Algorithm for Multi-Carrier Systems

Masahiro Fujii, Akihiro Waku, Makoto Itami, Yu Watanabe, Kohji Itoh

Orthogonal Frequency Division Multiplexing (OFDM) systems are very sensitive to the frequency offset of the local oscillator at the receiver. For the same reason, estimation of the frequency characteristics, needed for OFDM to be adapted to the frequency selective fading, can only be carried out conventionally after the frequency offset has been compensated. And accurate estimation of large frequency offset certainly requires high precision estimate of the frequency characteristics. In this paper, we propose a new joint estimation method of the frequency offset and the channel frequency response using an Expectation-Maximization (EM) algorithm for OFDM systems. The proposed algorithm overcomes the limitation of the thus far proposed algorithm. By computer simulations, we show the proposed algorithm provides estimation accuracy close to its lower bound in a wide range of the frequency offset.

Blind Matched Filter Method for Linear Frequency Modulated Pulse Radar

Fumio Nishiyama, Hideo Murakami

Linear frequency modulation has been used in air search radar primarily for pulse compression. Received signals observed by linear frequency modulated pulse radar are of target signals or clutter signals with different carrier frequencies. In several cases, received target data with different carrier frequencies have stronger correlation than clutter data has. In these cases, target data is assumed to follow the statistics of a Moving Average (MA) model, in spite of the fact that the statistics are not known in advance. The MA parameter is estimated from only the received data by the blind matched filter method. The matched filter is designed based on this estimated MA parameter. Signal-to-clutter Ratio is improved by this matched filter.

Detection Scheme for Burst Erasures in Magnetic Recording Channel

Masayuki Hayashi, Ryuji Kohno

In practical magnetic recording channel, burst erasures occur in addition to random error. It is well known that burst erasures are caused by thermal asperity (TA) and media defect (MD). In this paper, the detection scheme of the position of burst erasures is proposed. Proposed scheme utilizes the power monitoring of the read signal after equalization and calculates the erasure position and the erasure length. We show that the sequence estimation with viterbi algorithm using this burst erasure position and burst erasure depth as channel state information (CSI) outperforms the conventional scheme in perpendicular magnetic recording channels. Furthermore, we studied joint design schemes with error correcting code (ECC).

A Novel Equalization Algorithm for Frequency-Selective Channels

Peng Wang, Wee Ser

A common strategy to combat channel frequency selectivity is to implement an inverse filtering process at the receiver to recover the transmitted signal. This paper, however, introduces a different equalization algorithm. By adapting the decision rule to the time-varying inter-symbol interference, the proposed algorithm can provide satisfactory performance for a variety of channels.

Mon1-5 : Turbo Codes (1)

Performance Evaluation of High-Dimensional Parity Check Code with High Code Rate

Satoru Kose, Hiroshi Kamabe

The simplicity of encoding and decoding procedures of a code is an important factor when these procedures are implemented in practical systems. The structure of a high dimensional parity code with high code rate (HDPC$_{\boldsymbol{hc}}$) is very simple and there is a very simple hard decoding procedure. In this paper we show the performance of the code when we use the code as a constituent code for a iterated coding scheme by P. Elias and D. Rankin et al.

Study on Turbo Decoding Using Hard Decision Decoder – Principle of Hard-in Soft-out Decoding –

Kazuhiko Yamaguchi, Shinya Maehara, Brian M. Kurkoski, Kingo Kobayashi

We propose a new construction and decoding method for concatenated codes. One of the target coding schemes is a serially-concatenated coding scheme with a turbo code as the inner code and a Reed-Solomon (or other block) code as the outer code. The proposed decoding strategies include following two points. (1) New repetitive diagram of whole serial concatenated code is investigated. (2) To reduce complexity, hard-input soft-output decoding for the outer code is applied. Using a double error-correcting Reed-Solomon code as outer code, the results are evaluated and discussed.

Theoretical Analysis of Bit Error Probability for Convolutional Code with Max-Log MAP Decoding

Hideki Yoshikawa

In this paper, an analytical technique for bit error probability of 4-state convolutional code with Max-Log-MAP decoding is presented. This technique employs an iterative calculation of probability density function of state metric per a transition, and gives exact bit error probability for all SNR.

Modified EMLMAP Algorithm Using Variable Scaling Factor for Low-power Implemenation of Turbo Decoder

Jaebum Kim, Jaehong Kim, Byeongjo Kim, Seongsu Park, Hyuncheol Park

We propose a modified enhanced max-log-MAP (EMLMAP) algorithm using variable scaling factors (SFs) for low-power implementations of a Turbo decoder. We find the sub-optimum SFs $\hat{\alpha}$ which are quantized from 0.6 to 0.9 using extrinsic transfer characteristics (EXIT) analysis. Based on the analysis, the variation scheme of the SF is described, which is a function of half-iteration hard-decision-aided (HIHDA) early termination criteria S. Using computer simulations applying 8-state WCDMA Turbo codes of the rate $R = 1/3$ on memoryless binary-input continuous-output AWGN channel, we analyze the BER performance and average number of iterations of the proposed algorithm by comparing that of the conventional EMLMAP algorithm which is applied fixed SF and HIHDA early termination scheme. According to results of the simulations, the proposed algorithm has low-power efficiency and improvement in BER performance for a large interleaver of length $N > 3000$.

Mon2-1 : Coding Theory (2)

On the Correcting Property of a Two-dimensional Error-correcting Code Based on the Lee Metric on $\mathbb{Z}_{2^m}$

Banri Bannai, Manabu Hagiwara, Hideki Imai

A method for constructing Lee metric codes over arbitrary alphabet sizes and its decoding way is presented. This code is constructed without using the previously known techniques such as Galois rings and Gray map. In this paper, we introduce the code over $\mathbb{Z}_{2^m}$ and consider it when code length is 2. We find that whether m is even or odd is deeply concerned with the Lee-error-correcting property t. To know t is difficult when m is odd, however we find the way evaluating t from lower side over any $\mathbb{Z}_{2^m}$. We also show that the codes can correct error which exceeds t in some special cases, and that our decoding method approximates the bounded distance decoding when m is sufficiently small.

A Bound on q-ary t-EC-AUED Codes and Constructions of Some Optimal Ternary t-EC-AUED Codes

Irina Naydenova, Torleiv Kløve

Böinck and van Tilborg gave a bound on the length of binary t-EC-AUED codes. In this paper a generalization of this bound to arbitrary alphabet size is given. This generalized Böinck-van Tilborg bound, combined with constructions, is used to determine the length of some optimal ternary t-EC-AUED codes. An illustration of the the constructing method is given by constructing optimal ternary t-EC-AUED codes with size up to 9.

One Conjecture for Relationship between the Shift Bound and SchaubPlus Bound for Cyclic Codes

Junru Zheng, Takayasu Kaida

The Schaub bound is one of well-known lower bounds of the minimum distance for a cyclic code, and defined from its defining sequence. In 2003, this bound was improved and an algorithm for this improved bound called SchaubPlus bound was proposed by F.Ponchio and M.Sala. In this paper, we will claim one conjecture from numerical examples in binary and ternary cases.

Mon2-2 : Digital Right Management (2)

Digital Watermarking with Encrypted Watermarks by Using Masking Effects

Takahiko Oyachi, Kenji Nagasaka

In this note, we propose a method of embedding digital watermarks into digital still image keeping the quality of the embedded image. By using our method, the detection of embedded watermarks becomes harder, since they are encrypted. The encrypted digital watermarks are also converted into a certain code, with this code, the possibility of obtaining correct digital watermarks embedded against the overwriting and various destructions to the digital watermarking images. We need fairly

big number of bits to imbed digital watermarks and we make it possible to embedding bits by generalizing the idea of masking effects, which will be discussed else where.

Sanitizable Signature Scheme Applying Reversible Data Hiding

Minoru Kuribayashi, Masakatu Morii

When a document to be public contains the privacy or diplomatic information, such parts should be closed. However, a digital signature is attached with the document for the verification of the alteration on a digital document, no modification is allowed in general. The sanitizable signature scheme is one of the solutions which allows the conditional modification on the original document. In this paper, we proposed a new sanitizable signature scheme applying the reversible data hiding technique. In order to store the information concerning to closing parts of an original document, it is directly embedded into the disclosing parts of the document. Then generating a signature on such distorted and sanitized document, the integrity of both the document and the disclosing conditions determined by a sanitizer is assured in our scheme. Since the embedding operation is completely reversible, the original disclosing parts of the document can be recovered, hence the verification of the signer's signature is possible.

Provider Authentication for Bidirectional Broadcasting Service with Fixed Verification Key

Go Ohtake, Goichiro Hanaoka, Kazuto Ogawa

Several content distribution services via the Internet have been developed, and a number of bidirectional broadcasting services will be provided in the near future. To gain access to these services, a user must transmit personal information to a broadcaster through a network. This information may be leaked to a third party who impersonates the broadcaster, so provider authentication using a digital signature scheme is necessary to ensure the secure transfer of information. If the broadcaster's signing key is leaked to a third party, they could easily impersonate the broadcaster. To minimize damage caused by impersonation, we propose a content distribution system that enables secure provider authentication for bidirectional broadcasting services with fixed verification key even when a signing key is leaked. The system enables users to securely send personal information to the broadcaster while obtaining bidirectional broadcasting services.

Specifying the Subtree Number of a Content Distribution Tree Using Visual Cryptography

Hyunho Kang, Brian M. Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi

In our previous study, we have presented an approach for a video fingerprinting system. Recently, we have proposed some methods for generalization and considered tree specific and endbuyer specific problem under collusion attacks. In this paper, we use a visual cryptography scheme to minimize deterioration of tree-specific problem in our previous work. This approach is able to detect distinctly the logo image of our previous content distribution system even if the video content has been distorted by collusion attacks. In video fingerprinting system, collusion attacks such as averaging, maximum minimum, negative correlation and zero correlation collusion attacks are very powerful. Within the limits of a collusion attack on a single subtree, the attacked logo can be extracted. But if the collusion attack spans more than one subtree, distinctive logos are superimposed making it difficult to identify the subtrees of the colluding users. The technique proposed by Ateniese et al. (Extended VCC) will be the key to solve this problem in our opinion.

Subset Incremental Chain Based Broadcast Encryption with Shorter Ciphertext

Nuttapong Attrapadung, Hideki Imai

We propose a new efficient broadcast encryption scheme. Its ciphertext length is upper bounded by $2r$, the key size is $O(k \log n)$, and its computational cost is $O(kn^{1/k})$ for any parameter k; where r and n are the number of revoked users and all users respectively. This improves the ciphertext lengths from the previously best schemes, which were essentially forced to be $2kr$ in order to achieve sub-linear computational costs of $O(n^{1/k})$.

Mon2-3 : Shannon Theory (2)

A Class of Average Distributions for Monotone Sources

Mohammadali Khosravifard, Morteza Esmaeili, Hossein Saidi, T. Aaron Gulliver

In order to select a unique code for the class of monotone sources with N symbols one may use the minimum average criterion. It is known that the optimal code is the Huffman code for the expected symbol probabilities. In this paper, we consider the case when monotone sources with a higher kth symbol probability are more likely. Assuming a probability density function $f(p_1, p_2, \ldots, p_N)$, which is proportional to p_k^m for some $m \in \mathbb{N}$, a closed form expression for the expected symbol probabilities, i.e. $E_{k,m}(p_i)$ is presented. The Huffman code for the average probabilities is optimum from the minimum average redundancy point of view. Some properties of the average distribution, i.e. $(E_{k,m}(p_1), \ldots, E_{k,m}(p_N))$, are examined. Also, a minimax method for determining the appropriate value of the exponent m is proposed.

Information-Spectrum Characterization of a Multi-terminal Channel with General Correlated Sources

Ken-ichi Iwata, Yasutada Oohama

In this paper, Information-Spectrum characterizations are derived for the reliable transmission of correlated outputs from general sources over a general multi-terminal channel. We provide the necessary and sufficient conditions for the transmission of the given general sources over the given general channel by using Information-Spectrum methods which was introduced by Han and Verdú.

Source Coding of Correlated Gaussian Vector Sources with Several Side Informations at the Decoder

Yasutada Oohama

We consider the source coding of L correlated Gaussian sources $X_i, i = 1, 2, \cdots, L$. We consider the case where L noisy observations $Y_i = X_i + N_i$ of $X_i, i = 1, 2, \cdots, L$ work as partial side informations at the decoder. Distortion is measured by a covariance matrix with the difference between original L sources and their estimations. We derive explicit outer and inner bounds of the rate distortion region. We show that the above the outer bound coincides with the inner bounds when Gaussian correlated sources satisfy some conditions.

Multiterminal Source Coding with Complementary Delivery

Akisato Kimura, Tomohiko Uyematsu

A coding problem where messages from two correlated sources are jointly encoded and separately decoded is investigated. Each encoder has access to one of the two messages to enable it to reproduce the other message. The rate-distortion function for lossy coding is clarified. Some related coding problems are also examined.

Mon2-4 : Communication Systems

Modeling of Impulse Noise for Indoor Broadband Power Line Communications

Daisuke Umehara, Shinji Hirata, Satoshi Denno, Yoshiteru Morihiro

Residential power line is one of the most attractive communication media for in-home networking, since almost all rooms in a house have power outlets. The regulations on power line communication (PLC) may be eased in Japan and we could

utilize a frequency band from 2 to 30MHz in the future. However, many electrical appliances and/or shortwave systems frequently cause man-made electromagnetic interference on indoor power line. This man-made noise often has impulsive characteristics. We will extend knowledge about impulse noise at indoor power line in the frequency range from 2 to 30MHz. We measure indoor power line noise in several environments and apply a detection method by chi-square test to the measured noise. Further we model the amplitudes, durations, and interarrival time of indoor power line impulses. These impulse noise models are expected to utilize for communication design about PLC.

A Modulation Classification Analysis Using Joint Moments with Linear Transform

Daisuke Shimbo, Ikuo Oka, Shingo Ata

In adaptive modulation systems, a transmitter selects the best modulation from various signaling formats against time varying disturbances, and a receiver identifies the modulation using a received signal. In this paper, a modulation classification method based on joint moments using linear transform is proposed. In the method, the amplitude and phase of a received signal are transformed linearly, and joint moments are measured from the amplitude and phase. The moments depend on the linear transform, and the classification performance improves by some transforms. The joint moments are derived in a form of an infinite series of elementary functions to analyze an optimal decision threshold and a classification error probability. Numerical results of the classification error probability for BPSK, QPSK and 16QAM show the superiority of the proposed method with appropriate linear transforms.

Intersymbol Interference Compensation Scheme in Collaboration with Transmit Pre-coding and Adaptive Equalization

Hiroshi Kubo, Shinich Mochida, Katsuyuki Motoyoshi, Takashi Mizuochi, Akihiro Shibuya

This paper proposes a communication system employing precoding at a transmitter and adaptive equalization at a receiver, i.e., a collaborative equalization scheme. Assuming slowly time-varying and large time-span intersymbol interference (ISI) channels, e.g. hundreds of symbol duration, the proposed collaborative equalization scheme roughly compensates ISI by pre-coding at the transmitter and precisely compensates a residual ISI by adaptive equalization at the receiver. Computer simulation confirms that the proposed collaborative equalization scheme has excellent performance in the presence of large time-span ISI and residual ISI due to mismatch of pre-coding, assuming chromatic dispersion in optical communications.

Modified PN Code Acquisition Scheme Based on Adaptive Filter Under Frequency Selective Rayleigh Fading Channels

Donghoon Lee, Kyungwhoon Cheun, Jeongchang Kim

A hybrid PN code acquisition system based on a least-mean-square adaptive filter, interpreted as a channel estimator, is proposed for direct-sequence spread-spectrum systems under frequency selective Rayleigh fading channels. Closed form expressions for the detection and false alarm probabilities are derived. Compared to the previously proposed channel equalizer based system, the proposed system achieves smaller mean acquisition times and is more robust to the selection of the adaptation step-size. The proposed algorithm does not require multiplication operations for coefficient weight updates.

Mon2-5 : Turbo Codes (2)

Improvements and Extensions of Low-Rate Turbo-Hadamard Codes

Noriyuki Shimanuki, Brian M. Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi

In this paper, we consider a number of system improvements that have been proposed for convolutional turbo codes, and apply them to turbo-Hadamard codes (THC). Our findings are as follows. 1. Asymmetrical THC, employing differing constituent codes, improves the waterfall region performance compared to symmetrical THC. 2. Punctured THC have improved performance in both the waterfall and error floor regions, relative to non-punctured codes of the same rate. 3. An LDPC code, when serially concatenated with an inner THC code, can correct low weight errors to improve the error floor performance. 4. Parallel-schedule decoding of THC can converge significantly faster than conventional serial-mode decoding, leading to a reduction in decoder complexity.

Interleaver Design for a Class of High-Rate Serially Concatenated Codes

Motohiko Isaka

This paper discusses an interleaver design for a class of serially concatenated coding schemes with relatively short linear outer block codes and an inner accumulator encoder. It is shown that an appropriate design of an interleaver enhances the performance of the error floor, in which the associated error events are not entirely due to the existence of low-weight codewords.

Stopping Sets for Iterative Row-Column Decoding of Product Codes

Eirik Rosnes

In this work we introduce stopping sets for iterative row-column decoding of product codes using optimal constituent decoders. Let C_p denote the product code of two binary linear codes C_c and C_r of minimum distances d_c and d_r and second generalized Hamming weights $d_2(C_c)$ and $d_2(C_r)$, respectively. We show that the size $s_{\min}$ of the smallest non-codeword stopping set is at least $\min(d_r d_2(C_c), d_c d_2(C_r)) > d_r d_c$, where the inequality follows from the Griesmer bound. If there are no codewords in C_p with support set $\mathcal{S}$, where $\mathcal{S}$ is a stopping set, then $\mathcal{S}$ is said to be a non-codeword stopping set. We also give an explicit formula for the number of non-codeword stopping sets of size $s_{\min}$, which depends only on the first non-zero coefficient of the constituent (row and column) first and second support weight enumerators, for the case when $d_2(C_r) < 2d_r$ and $d_2(C_c) < 2d_c$. An immediate consequence is that the erasure probability after iterative row-column decoding of (finite-length) product codes on the binary erasure channel approaches the erasure probability after maximum-likelihood decoding as the channel erasure probability decreases. Finally, as an example, we apply the derived results to the product of two (extended) Hamming codes and two Golay codes.

The Double Binary Turbo Hybrid ARQ Scheme

Woo Suk Kwon, Jeong Woo Lee

In this paper, we propose an incremental redundancy(IR)-hybrid ARQ (HARQ) scheme which uses double binary turbo codes for error correction. The proposed double binary turbo IR-HARQ scheme provides higher throughput than the IR-HARQ, which uses binary turbo codes for error correction, at all E_s/N_0. An extra coding gain is also attained by using the proposed HARQ scheme over the coding gain achieved by turbo codes only.

Tue1-1 : Coding Theory (3)

Optimality on Probabilistic Minimax Robust Decoder

Libo Yang, Lei Wei

In this paper we show the minimax robust decoder in [10] is actually optimal in term of minimizing the worst case bit error probability for channels with two-type noise model with unknown prior probabilities. We prove that the decoder based on minimax rule is actually not affected by prior probabilities of the noise model, which means average bit error probability a constant, regardless of prior probabilities of the noise model. An example is given to illustrate the results.

A Comparison between WB Algorithm and BM Algorithm

Shojiro Sakata, Masaya Fujisawa

Before, we presented dualistic extensions of the Berlekamp-Massey (BM) algorithm, i.e. for multiple arrays and for array vectors. The former extension which is equivalent to the Feng-Tzeng algorithm can be applied to decoding of BCH codes up to Hartmann-Tzeng bound, but the latter remained to be applied to any significant decoding of RS codes or other algebraic codes. In this paper we show that the vector-version of BM algorithm is useful in solving the Welch-Belekamp (WB) key equations for decoding of RS codes as an alternative of the WB algorithm. Both methods have the same computational complexity.

On Behavior of RS-decoder Based on Welch-Berlekamp Algorithm for $t + \mu$ Errors

Masami Mohri, Masakatu Morii

When $(t + \mu)$-error is occurred on a codeword of t-error-correcting Reed-Solomon code, it has been shown some cases such that the candidate vector generated by RS decoder (based on the Euclidian algorithm and Peterson algorithm) is not a codeword. These cases are called decoder-malfunction. However, the behavior of decoder-malfunction for Welch-Berlekamp algorithm has not been shown. In this paper, we show the condition for decoder-malfunction of Welch-Berlekamp algorithm. Furthermore, we show some consideration about candidate vectors obtained by decoder-malfunction of WB-algorithm.

An Improvement to an Iterative Bounded-distance and Encoding-based Decoding Algorithm for Binary Linear Block Codes

Hitoshi Tokushige, Marc Fossorier, Toru Fujiwara, Tadao Kasami

We proposed an effective selection method of test patterns for an iterative decoding algorithm using bounded-distance and encoding-based decodings of binary linear block codes. Simulation results show that the iterative decoding algorithm using the selected test patterns (IDA) provides considerably better error performance than conventional iterative decoding algorithms with the same number of iterations. In this paper, we present simulation results of decoding complexity of the IDA with an early termination condition for the BCH(127, 64, 21) code over an additive white Gaussian noise channel using binary phase shift keying modulation. The results show that the early termination condition reduces a large number of iterations. Hamming distance distributions between transmitted codewords and the decoded codewords of the IDA are also shown by computer simulation. We give a suggestion for improvement of error performance of the IDA based on the distributions.

Method for Generating a Competing Codeword Using a Chain of Minimum Distance Searches

Jun Asatani, Takuya Koumoto, Toru Fujiwara, Tadao Kasami

In list-based soft-input soft-output decoding algorithms, two codewords are necessary to calculate a soft-output value at each bit position, that is, the most likely codeword and a competing codeword. We have proposed a list-based soft-input soft-output decoding algorithm using minimum distance search, which finds a competing codeword effectively except for low SN ratios. However, from a survey of the distribution of the Hamming distance between the most likely codeword and the competing codeword, which are generated by maximum likelihood decoding algorithm, it turned out that there were not negligible competing codewords at second or further Hamming distance from the most likely codeword for relatively low SN ratios. In this paper, a method is proposed for generating a competing codeword by using a chain of minimum distance searches to find a competing codeword at further Hamming distance from the most likely codeword. By computer simulation, the proposed method is shown to be capable of generating competing codewords more accurately than the previous one.

Tue1-2 : Network Security

A New Secret Key Agreement Scheme Based on Eigenvalues of Channel Matrices in Phase-Controlled MIMO Systems

Kengo Hiwatashi, Hideki Ochiai, Junji Shikata

In this paper, a new secret key agreement scheme is proposed for land mobile communications. This scheme generates a pair of secret key on both sides of two legitimate users by the use of eigenvalues of channel matrices similar to the existing work, but without making use of reciprocity of radio wave propagation. The simulation results show that the proposed scheme maintains robustness against a mismatch in term of channel reciprocity.

A Study on Detection of Varied Worms with Analyzing Session Information

Il-Ahn Cheong, Taek-Yong Nam

Since many worm attacks appear, more and more varied worms have become a threat to our networks. In this paper, we study to detect these varied worms with analyzing session information from a worm data. We use the session information of a network dump data generated by worm attack and the automatic generation method to generate detection rules that is adequate to find peculiar rules of worm based on entropy theory. As the result, we are able to automatically generate the detection rules of worm attacks and to effectively detect varied worms with the rules.

Reliability Improved Port Knocking Scheme

Hiroyuki Tanaka, Takashi Katoh, Bhed Bahadur Bista, Toyoo Takata

Port knocking is a method of communication in which information is encoded into a sequence of port numbers, and is regarded as the most promising method to realize remote authentication in a mobile environment.

In this paper, we propose a new port knocking scheme especially suitable for wireless environment. Our proposed scheme employs interleaving and erasure-correcting coding to combat a packet loss before establishing connection.

An IP Traceback Scheme with Variably Probabilistic Packet Marking

Takeaki Terada, Masakazu Soshi, Atsuko Miyaji

One of the effective countermeasures against Denial of Service (DoS for short) attacks is IP traceback, which tries to identify the attacker by determining the attack path. In particular Probabilistic Packet Marking (PPM) for IP traceback is so promising that many researches on it have so far been done. However, most of the previous PPM schemes have the disadvantage such that they require a large number of packets to reconstruct the attack path. Therefore we propose an efficient traceback scheme based on PPM in this paper.

Implementation and Evaluation of Dynamic Process Resolution Protocol Actualizing Location Transparency

Hidekazu Suzuki, Akira Watanabe

In order to realize secure communications in an enterprise network, an effective way is to form communication groups corresponding to different types of tasks. However, based on traditional forming methods, it has been difficult to realize an effective system because a management load increases in the environment where individual-based and unit-based communication groups coexist or when dynamic adjustment to changes in the network configuration is needed. Thus, we have been proposing the concept of Flexible Private Network (FPN) that provides both flexibility and security. Dynamic Process Resolution Protocol (DPRP) is a protocol that can actualize Location Transparency. In DPRP, all devices existing in the communication path mutually exchange information in advance of communication, and create Process Information Table

(PIT) which is needed for communication between terminals in each device. We have implemented DPRP in the IP layer on FreeBSD and confirmed that the overhead of DPRP does not affect on TCP/UDP communications. We have also proved that a management load can be reduced drastically.

Tue1-3 : Source Coding

Universal Lossy Coding for Individual Sequences Based on Complexity Functions

Shigeaki Kuzuoka, Tomohiko Uyematsu

A theory of lossless compression of individual sequences has been formulated by Ziv and Lempel, and developed by their subsequent papers. While the framework of lossless coding problem of individual sequences can be extended to lossy coding problem, the lossy coding problem of individual sequences are not so well studied as the lossless coding problem. This paper considers four kinds of rate-distortion problems for individual sequences: the fix-rate coding under the maximum-distortion criterion (fm-coding) and the average-distortion criterion (fa-coding), the variablerate coding under the maximum-distortion criterion (vm-coding) and the average-distortion criterion (va-coding). The converse coding theorems for each problem are established. Moreover, universal lossy coding schemes for individual sequences based on the complexity function are proposed, and the coding theorems for fm, fa and vm-coding problems are clarified.

On the Optimum Performance Theoretically Attainable for Scalarly Quantized Correlated Sources

Thorsten Clevorn, Laurent Schmalen, Peter Vary, Marc Adrat

Turbo processing enables appropriately designed systems to operate close to their capacity limits. In this contribution we present an upper bound, the optimum performance theoretically attainable (OPTA), that can be achieved when transmitting the samples of scalarly quantized correlated sources. This OPTA limit is based on the combination of the channel capacity and and the distortion rate function. To incorporate the effects of the finite block sizes in real systems, additionally the inevitable loss is taken into account by the sphere-packing bound. In a simulation example we present a multi-mode iterative source-channel decoding scheme that is based on highly redundant index assignments. By its Turbo processing at the receiver and due to its multi-mode flexibility this system can approach the OPTA limit in a wide range of channel conditions.

Bounds on Exponentiated Expected Length of Optimal Binary Prefix Codes

Yen-Yi Lee, Jay Cheng

In this paper, we consider the exponentially weighted average codeword length introduced by Campbell, which assumes that the cost is an exponential function of the codeword length and includes the usual expected codeword length as a special case. Such situations could arise when the cost for encoding and decoding is significant, or if the buffer overflow caused by long codewords is a serious issue. Under Campbell's average codeword length criterion, we derive some properties of optimal binary prefix codes, and obtain new lower and upper bounds on the exponentiated expected length of optimal binary prefix codes when the probabilities of the most and/or the least likely source symbols are available.

Improving LZ77 Data Compression Using Bit Recycling

Danny Dube, Vincent Beaudoin

Many data compression techniques allow for more than one way to encode the compressed form of data. In particular, this is the case for the LZ77 technique and its derivatives, where matches can often be described in more than one way. The very existence of multiple encodings for the same data acts as a side-channel through which additional information can be conveyed from the compressor to the decompressor, and so, for free. We show that this side-channel can be used to carry parts of the compressed file itself, thereby shortening the latter, and improving compression ratios. We call our technique *bit recycling* and show how it applies to Huffman encoding. We present it as a way to improve LZ77 compression and demonstrate it through many experiments. One of these experiments has already been presented but the new ones take better advantage of recycling. The experiments show that we can improve compression efficiency significantly and tend to point to a method with which bit recycling is most profitable.

Linear-Time Encodable and Decodable Codes for Slepian-Wolf Source Networks

Tomohiko Uyematsu

This paper proposes an explicit construction of fixed length codes for Slepian-Wolf source networks. The proposed code can be encoded and decoded in linear time. Our construction of the code is similar to the error correcting code proposed by Guruswami and Indyk for channel coding, and the code has iterative decoding procedure. It is shown that the probability of error vanishes exponentially as the block length tends to infinity, if the pair of encoding rates is in the achievable region of the correlated source.

Tue1-4 : Spread Spectrum Systems

Impact of Narrowband Interference for DS-multiband-UWB Wireless Communications

Yun-Seok Song, Shigenobu Sasaki, Chin Sean Sum, Hisakazu Kikuchi

This paper presents the simulation results of a direct sequence ultra wideband (DS-UWB) communication system applying multiband modulation over multipath wireless channel in the presence of narrowband interference. Simulation results of system performance are presented corresponding to different chip duty factor and signal to interference ratio (SIR). We found that system performance can be improved significantly by decreasing chip duty factor.

On Interference Mitigation of DS-Multiband-UWB System Over Indoor Multipath Environment

Chin Sean Sum, Shigenobu Sasaki, Hisakazu Kikuchi

This paper presents the interference mitigation capability of a hybrid direct sequence (DS) multiband (MB) ultra wideband (UWB) system with Rake receiver over indoor multipath environment. By suppressing the power of the particular sub-band affected by coexisting narrowband or wideband interference, the impact of interference can be reduced significantly. Theoretical analysis is conducted to investigate this interference mitigation capability corresponding to various system parameters such as level of power suppression, signal to noise ratio, signal to interference ratio, number of employed bands and interference signal bandwidth. We found that by suppressing the sub-band power, system performance can be improved while maintaining the processing gain.

Short and Efficient Frequency Hopping Sequences

Young-Joon Kim, Dae-Son Kim, Hong-Yeop Song

This paper is about designing a short hopping sequence. Because of short length, we have only to consider balance and Hamming autocorrelation. Modulo q reduction of consecutive powers of a primitive root $\mu \pmod p$ and deleting a position at a given q-ary power residue sequence of period p are proposed as a design of q-ary sequence of period $p-1$, where p is a prime. These sequences are compared in terms of Hamming autocorrelation and balance.

Throughput Performance of the MPPM DS/SS ALOHA System on the AWGN Channel

Masayuki Matsuzaki, Fumie Ono, Hiromasa Habuchi

In this paper, the throughput performance of the Multipulse Pulse Position Modulation Direct Sequence/Spread Spectrum (MPPM DS/SS) ALOHA system is evaluated on the AWGN

channel. In the MPPM DS/SS ALOHA system, information data are represented by combination the slot positions of several spreading codes and the sign in a packet. Therefore, this system can reduce interferences of other users by decreasing the number of spreading codes per packet. The packet length of the MPPM DS/SS ALOHA system is shorter than that of the DS/SS ALOHA system. As a result, throughput performance of the MPPM DS/SS ALOHA system is about 2.3 times larger than that of the DS/SS ALOHA system, about 1.3 times larger than that of the ALOHA system applied with three-valued signaling.

Construction of Continuous-Time Equivalents of Welch Bound Equality Sequences

Joon Ho Cho

Recently, the Welch bound equality (WBE) sequences and their variations have been intensively investigated for applications to code-division multiple-access (CDMA) communications and, accordingly, many algorithms to construct these sequences have been proposed. In this paper, we propose an algorithm called multi-user piecewise-constant constrained water-filling to construct the continuous-time equivalents of Welch bound equality (CTE-WBE) sequences, which are continuous-time counterparts of the WBE sequences.

Tue1-5 : MIMO (1)

Communication over Hypercomplex Kähler Manifolds: Capacity of Dual-Polarized Multidimensional-MIMO Channels

Özgür Ertuğ

We consider single-user communications over joint space-pattern-polarization diversity providing dual-polarized multidimensional-MIMO (MD-MIMO) channels established by the use of multiple dual-polarized transmit/receive antennas in the form of uniformly-spaced 1D, 2D and/or 3D MIMO arrays. Based on the equivalent channel-models formulated based on hypercomplex Kähler manifolds, we subsequently identify the decomposition of dual-polarized multidimensional-MIMO channels into multiple independently-fading and scaled classical MIMO channels in parallel through the algebraic properties of hyperKähler manifolds and consequently derive the corresponding ergodic capacities analytically. We show in essence via the diversity-reception over independent channels perspective deduction of the decomposition into parallel MIMO channels observation that the capacity gains achievable by dual-polarized multidimensional-MIMO Tx/Rx over classical single-polarized linear antenna array MIMO Tx/Rx may be notably large with equal number of transmit and/or receive antenna locuses constrained compactly and under same resource requirements/channel conditions whenever the cross-polar discrimination is good, i.e. $\rho \ll 1$.

Transceiver Optimization for Multiuser MIMO Systems: Min-Max Relative User-MSE under a Total Power Constraint

Shuying Shi, Martin Schubert, Holger Boche

We address the problem of jointly optimizing linear transmit and receive filters for a multiuser MIMO system, under the assumption that all users have individual minimum mean square error (MMSE) requirements. The design goal is to minimize the maximum relative MSE per user under a total power constraint. This results in a non-convex problem formulation. We propose an iterative algorithm which performs optimization in an alternating manner by switching between the uplink and downlink channel. The proposed algorithm has very low complexity and fast convergence behavior. We prove that the balanced relative user-MSE level returned by the iteration decreases monotonically and converges. Furthermore, the proposed algorithm has no restriction on the number of transmit and receive antennas.

Selecting a Near-Optimal Set of Joint Transmit-Receive Antennas for a MIMO Channel Based on Maximizing Channel Capacity

Hyo-Shil Kim, Sung-Yeon Kim, Youn-Shik Byun

Increasing the number of transmit and receive antennas are required for higher hardware costs and computational burden in multiple input multiple output wireless systems. For systems with a large number of antennas, there is strong motivation to develop techniques with reduced hardware and computational costs. In this paper, we propose an efficient transmit-receive antenna selection algorithms for MIMO wireless systems. Our algorithm achieves the more near ergodic capacity as the optimal selection technique than existing nearly optimal antenna selection schemes. We present the proposed algorithms that tractable linear algebra analysis of channel capacity. Simulations validating analysis and illustrating the proposed algorithms performance are also presented.

On the Complexity of Feedback Generation in MISO Beamforming and Diversity Schemes

Albrecht J. Fehske, Patrick Marsch, Gerhard P. Fettweis

Recently, different schemes have been introduced that improve the bit error rate of single user MISO transmissions through transmit diversity or transmitter-sided beamforming. This is particularly interesting in the downlink of cellular systems, where it is feasible to employ multiple transmit antennas at the base stations, but only few receive antennas at the mobile terminals. In this paper, we observe both classical beamforming schemes, where a beamforming vector is chosen to optimize the SINR at the receiver, and Coherent Alamouti schemes, which extend the classical rate one Alamouti STBC to multiples of two transmit antennas. In both cases, full diversity and an additional gain can be achieved, if a certain extent of channel knowledge is present at the transmitter, which usually has to be supplied by the receiver through feedback. In our work, we evaluate the performance and feedback requirements of the different schemes, while putting a special emphasis on the non-negligible computational complexity required at the receiver to produce optimal feedback. We introduce a novel beamforming scheme that can significantly reduce this complexity while achieving a comparable performance, and provide a comprehensive summary on the choice of an optimal transmission scheme for different applications.

Tue2-1 : LDPC Codes (1)

A Minimum Weight Test for a Certain Subclass of Array LDPC Codes

Kenji Sugiyama, Yuichi Kaji

LDPC codes is a class of linear codes introduced by Gallager in early 60's. Array LDPC (ALDPC) codes is a class of LDPC codes which are algebraically constructed from a family of array codes. This paper proposes a procedure to check if there is a codeword with specified weight in a certain ALDPC code. The minimum weight of a linear code has strong relationship to the performance of the code, but unfortunately it is difficult to compute the exact minimum weight of long and randomly constructed LDPC codes. We restrict ourselves to a class of complete array LDPC codes (C-ALDPC codes) which is a subclass of array LDPC codes, and investigate positions of nonzero components in a codeword. The code in the considered subclass is invariant under a doubly transitive group of affine permutations. This property gives significant constraint on the positions of nonzero components in a codeword, which means that the positions of nonzero components in a codeword can be classified into rather small number of patterns. Using these conditions, the proposed procedure checks if there exists a codeword with specified weight.

On Minimal Length of Quasi Cyclic LDPC Codes with Girth ≥ 6

Manabu Hagiwara, Koji Nuida, Takashi Kitagawa, Marc Fossorier, Hideki Imai

In this paper, we investigate the smallest value of p for which

a (J, L, p) QC LDPC code with girth 6 exists for $J = 3$ and $J = 4$. For $J = 3$, we determine the smallest value of p for any L. For $J = 4$, we determine the smallest value of p for $L \leq 31$. Furthermore we provide examples of specific constructions meeting these smallest values of p.

Use of Dynamic Programming for the Design of Irregular LDPC Codes

Sang Hyun Lee, Duho Rhee, Il Mu Byun, Kwang Soon Kim

A simple design method using dynamic programming is proposed for good LDPC codes with relatively low code-rate. By applying a dynamic programming optimization to the construction of the portion fixed for easy encoding in the parity-check matrix, we can maximize the girth associated with columns contained in that portion of the matrix. Simulation results show performance improvement over the conventional controlled random construction method.

New Bit Mapping Scheme of Irregular LDPC Codes for Nonuniform Gaussian Channels

Hyeong-Gun Joo, Song-Nam Hong, Dong-Joon Shin

In this paper, we propose a mapping scheme to assign the codeword bits of irregular LDPC codes to nonuniform Gaussian channels. Contrary to the previously known mapping schemes such as mapping the codeword bits in consecutive order and mapping the information bits to more reliable channel, the proposed scheme flexibly maps the information and parity bits of codewords by considering the characteristics of code and channel such as degree distributions and channel gap. The proposed mapping scheme select the best bit mapping for the given environment, while keeping the same overall system complexity. For the various irregular LDPC codes and nonuniform Gaussian channels, the best mappings are derived and the validity of them is confirmed through simulation.

Tue2-2 : Data Security

Perfect $(2, n)$ Threshold Secret Sharing Systems Based on Binary Matrices with Constant Column Weight

Todorka Alexandrova, Hiroyoshi Morita

In this paper we propose a construction of $(2, n)$ threshold secret sharing systems using the generalized vector space construction based on matrices over $GF(2)$ with constant column weight. For this constraint on the matrices, we present lower and upper bound on the size of the shares for each user and a lower bound on the number of rows in the matrices assigned to each user.

A principal problem in the generalized vector space construction is the practical construction of the matrices that define the secret sharing scheme. Adding the constraint of constant column weight in the matrices, allows us to present a practical algorithm, which constructs recursively a set of matrices with constant column weight, that is suitable to define a $(2, n)$ threshold secret sharing scheme. The detailed steps in this algorithm are described in this paper.

For good practical implementation we would like to increase the number of users in the secret sharing scheme as many as possible. For this purpose the problem of calculating the maximum number of users in the secret sharing scheme has been studied in the paper. The proposed construction algorithm gives a lower bound on the maximum number of users that are able to joint the secret sharing scheme.

Collision-Controllable Hash Function

Hidenori Kuwakado, Masakatu Morii

This paper proposes a one-way hash function such that resistance to a collision is controllable, called a collision-controllable hash function. Specifically, the collision-controllable hash function is characterized by the property that it is easy to find a collision for any $c - 1$ inputs but it is hard to find a collision for any c inputs. The collision-controllable hash function can be constructed by using an ordinary collision-resistance hash function. Applications of the collision-controllable hash function include sanitizable signature schemes and chameleon commitment schemes.

A Cache Attack on SEED

Yoshitaka Ikeda, Takenori Ichikawa, Toshinobu Kaneko

SEED is a 128-bit block cipher with 128-bit key developed by Korea Information Security Agency in 1998. We propose a cache attack for SEED, which reveals 128-bit secret key with data complexity of $2^{28.6}$. In general, cache attack reveals round key, we analysed key scheduling process of SEED to determine the secret key. There are 128 bits round key for two rounds. It means that the effective key space size is 2^{120} for the key. It may seem some weakness for the key schedule of SEED.

A Categorizing-Guessed-Values Approach for the Key Recovery Attack against WEP

Toshihiro Ohigashi, Yoshiaki Shiraishi, Masakatu Morii

Wired Equivalent Privacy (WEP) protocol is a security protocol for wireless LAN communication. Recently, a lot of key recovery attacks against WEP were proposed, and the methods to improve those attacks were proposed too. In this paper, we propose a new method to increase the success probability of the key recovery attack. Our method can improve the key recovery attack even at the parameters that other methods cannot. Additionally, we confirm that the key recovery attack applying our method can work effectively against secure WEP implementation proposed by Yoshida et al.

A Method for Checking the Parity of $(\#J_C - 1)/2$

Masataka Akane, Yasuyuki Nogami, Yoshitaka Morikawa

This paper especially deals with genus two hyperelliptic curves in the form of $H(x, y) = f(x) - y^2 = 0$, where $f(x)$ is an irreducible polynomial of degree 5 over the prime field F_p. Using shift product-based polynomial transformation (SPPT), we propose a method to check the parity of $(\#J_C - 1)/2$, where $\#J_C$ is the order of hyperelliptic curve. Then, especialy for the hyperelliptic curves in the form of $H(x, y) = x^5 + a - y^2 = 0 \quad , a \in F_p$, this paper shows that the proposed parity check can be carried out only by two exponensiations over the prime field F_p.

Tue2-3 : Shannon Theory (3)

Channel Coding Theorem for Discrete Multipath Channel

Yoichiro Watanabe, Koichi Kamoi

A channel coding theorem is proved for a discrete multipath channel (DMPC), which is a single-input, single-output discrete channel with memory. Memory in DMPC is induced by feedforward delay devices. A rate less than maximum value of the conditional mutual information of a multiple-access channel is an achievable rate for the DMPC.

Outage Behavior of Discrete Memoryless Channels Under Channel Estimation Errors

Pablo Piantanida, Gerald Matz, Pierre Duhamel

Classically, communication systems are designed assuming perfect channel state information at the receiver and/or transmitter. However, in many practical situations, only an estimate of the channel is available that differs from the true channel. We address this channel mismatch scenario by introducing the notion of estimation-induced outage capacity, for which we provide an associated coding theorem and its strong converse, assuming a discrete memoryless channel. The transmitter and receiver strive to construct codes for ensuring reliable communication with a quality of service (QoS), in terms of achieving a target rate with small error probability, no matter which degree of accuracy channel estimation arises during a transmission. We illustrate our ideas via numerical simulations for transmissions over Ricean fading channels using rate-limited feedback channel and maximum likelihood (ML) channel esti-

mation. Our results provide intuitive insights on the impact of the channel estimate and the channel characteristics (SNR, Ricean K-factor, training sequence length, feedback rate, etc.) on the mean outage capacity.

Improved Bounds for the Capacity of the Binary Deletion Channel

Hugues Mercier, Vijay K. Bhargava

We consider the deletion channel, where each transmitted bit is deleted with probability p_d, and present two computational methods to estimate its capacity. The first approach bounds the mutual information between the input and the output of the channel. It converges from above as the size of the input blocks approaches infinity and leads to the first nontrivial upper bound for the capacity. The second method uses stochastic optimization to maximize the information rate of the channel when the input source is modeled by a Markov process. It converges from below as the order of the optimal Markov chain increases, and as a result we improve on the existing capacity lower bounds.

Tue2-4 : UWB

Effect of Multi-path on Rake Reception for UWB-IR Communications

Isamu Matsunami, Keiji Terasaka, Kenji Higashikatsuragi, Akihiro Kajiwara

UWB-IR communications have attracted considerable attention because of their multi-path mitigation and system simplicity. Also the performance can be improved using the Rake combining of multiple paths. However the performance might be affected by the correlation loss with its template waveform where the transmit waveform is used as the template waveform. Especially in OLOS and NLOS channels the received signal waveform should be distorted by multi-path interference. In this paper we conducted various UWB-IR channel measurements and the signal distortion by multi-path interference is investigated. Also the Rake gain and energy capture are estimated.

Experimental Evaluation of In-home UWB-IR Propagation Characteristics

Keiji Terasaka, Kenji Higashikatsuragi, Isamu Matsunami, Akihiro Kajiwara

In this paper, the feasibility of human movement being detected is discussed, aiming at a Ultra-wideband Impulse-radio(UWB-IR) based home security sensor to protect a house, not a room like infra-red and conventional microwave sensor, from intruders. Measurement of the UWB-IR channels was conducted inside a house with four rooms including a living room where the transmit and receive antennas were placed in a fixed position of different rooms respectively in order to cover over the house. Measurement was conducted over all the floors with 365 locations and the power delay profiles are discussed in order to investigate the feasibility of human movement being detected. From the measurement results, the channel sensing based on UWB-IR is found to be useful to protect a home from intruder.

Optimality of Modulated Hermite Pulses for UWB/PPM Systems

Burak Berksoy, Lei Wei

In this paper we compare the modulated Hermite pulse, which is proposed for UWB/OOK communication systems (802.15-03) and optimal pulse waveforms developed for UWB/PPM. We show the hermite pulse is practically optimal when we select correct modulation index. This means if the future UWB system selects PPM modulation scheme instead of OOK, then the performance can be substantially improved without changing pulse waveform. On Gaussian-channels, the gain is 2.963dB over OOK and 0.838dB over PPM with conventional gaussian derived pulse.

Multi-Band Ultra-Wide Bandwidth Data Transmission Using Raised Cosine Pulse Shaping

Chaiyaporn Khemapatapan

In this paper, quadrature-phase shift-keying (QPSK) modulation and time hopping spread spectrum technique are applied to impulse radio signals for transmission data in an ultra-wide bandwidth (UWB) system. The proposed system takes an advantage of transmission carrier with pulse shaping in order to ease the design and implementation of transmitter and receiver using digital devices. Raised cosine filter is used as a pulse shaper. The transmitted signal consists of multi-band UWB signals in order to make spectrum to be efficiency and to enhance data transmission rate. By using raised cosine pulse shaping, the proposed system can be easily and partly implemented by digital devices.

A Simple Non-Coherent Detector for OOK on UWB Channels

Burak Berksoy, Lei Wei

In this paper, we introduce and evaluate two noncoherent detectors for UWB channels. The bit error performance is compared with the optimal coherent receiver and the energy detector. Different pulse waveforms are evaluated and bandwidth of transmitter and receiver filters are also optimized. The results show that on Gaussian channels , one of detectors not only achieves a performance better than the energy detector, but also requires much less computation complexity if implementing in DSP chips. On UWB channels, the performance is comparable with the energy detector, however, the circuitry is much less complex.

Tue2-5 : MIMO (2)

Influence of Transmit and Receive Correlations on Performance of the MIMO System with Multiple Antennas and Relay Terminals

Ryosuke Uchida, Hiraku Okada, Takaya Yamazato, Masaaki Katayama

In this manuscript, spatial diversity for in-factory environments is considered. The proposed scheme uses multiple antennas at a transmitter and a receiver, and also multiple relay terminals to provide diversity gain against fading and shadowing. If the separation of antennas at the transmitter or the receiver is not enough, then diversity gain is influenced by correlation at the transmitter or the receiver. This manuscript shows the analytical and numerical results of the effects of transmit and receive correlations on bit error performance of the proposed spatial diversity scheme.

On Iterative Decoding in Multiuser Space-Time Coding Systems

Ha H. Nguyen, Yajun Yang, Ed Shwedyk

In iterative receivers of bandwidth-efficient multiuser space-time block coding systems, the extrinsic information can be iteratively exchanged among the soft-input soft-output (SISO) channel decoders, the SISO multiuser detector and the SISO M-ary demodulators. This paper investigates and compares the performance of such receivers when different strategies of exchanging the extrinsic information are implemented. It is shown that the receiver that runs two inner iterations (between the channel decoders and the M-ary demodulators) for every one outer iteration (between the channel decoders and the multiuser detector) is the most attractive when taking into account the error performance, receiver complexity and decoding delay.

Sphere Decoder for Imperfect Channel State Estimation

Chimato Koike, Ryutaroh Matsumoto, Tomohiko Uyematsu

In the multi-antenna communication, it is usually necessary to estimate the channel state information(CSI). However, it is difficult to estimate CSI perfectly. We propose an algorithm

that effectively finds the most likely transmitted signals with the imperfect CSI. The computer simulation shows that the proposed method improves the symbol error rate and reduces the required number of the pilot symbols.

Multirate Multiuser Code for Multiple-Access Adder Channel

Jun Cheng, Koichi Kamoi, Yoichiro Watanabe

Multiuser error-correcting code for multirate data transmission is proposed for multiple-access adder channel (MAAC). By spreading sequences, chosen among tree-structured spreading sets, with different lengths and with decodability, data transmission is carried out at different rates. This satisfies the multirate requirement in multiple-access communication system, even if there exits channel noise.

Tue3-1 : LDPC Codes (2)

Complete Erasure Recovery of Irregular Repeat-accumulate Codes

Saejoon Kim

We consider the problem of complete erasure recovery of irregular repeat-accumulate codes used over the binary erasure channel. Elaborating on the properties of expander graphs, we give an extended construction of irregular repeat-accumulate codes that complete the recovery of all erasures and as a result, achieve the channel capacity.

Cycle Analysis and Interleaver Design of Finite-Length Punctured LDPC Codes with Dual-Diagonal Parity Structure

Yong Chun Piao, Dong-Joon Shin

In this paper, we analyze the cycle structure of finite-length punctured RA-type LDPC codes and design interleavers which have good memory efficiency and avoid short cycles. Furthermore, introduce the check-node merging scheme for finite-length punctured RA-type LDPC codes and design simple interleavers. Simulation results show that finite-length punctured RA-type LDPC codes using the proposed simple interleavers have better performance than those with random and S-random interleavers.

Analysis of Generalized LDPC Codes with Random Component Codes for the Binary Erasure Channel

Enrico Paolini, Marc Fossorier, Marco Chiani

In this paper, a method for the asymptotic analysis of generalized low-density parity-check (GLDPC) codes on the binary erasure channel (BEC) is proposed. The considered GLDPC codes have block linear codes as check nodes. Instead of considering specific check component codes, like Hamming or BCH codes, random codes are considered, and a technique is developed for obtaining the expected check EXIT function for the overall GLDPC code. Each check component code is supposed to belong to an expurgated ensemble. Some GLDPC thresholds obtained by this technique are compared with those of GLDPC codes, with the same distribution and component codes lengths, using specific codes. Results obtained by combining our analysis with differential evolution tool are also presented.

Performance of Low-Density Parity-Check Codes for Burst Erasure Channels

Gou Hosoya, Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa

Performance of low-density parity-check (LDPC) codes with maximum likelihood decoding (MLD) for solid burst erasures is discussed. The columns of the parity-check matrix of LDPC codes are permuted to increase the distance between elements (DBEs) which is defined as a number of symbol positions between elements 1 at each row of the parity-check matrix. The column permutation method can change the burst erasure correction capabilities by both the sum-product decoding algorithm and MLD algorithm. We derive some properties and show from simulation results that large values of DBEs leads to good performance for MLD.

Concatenated Coding System with Array and LDPC Codes for Burst-Error Channel

Hidetoshi Saito, Masayuki Hayashi, Ryuji Kohno

It is shown that the maximum a posteriori decoding with an autoregressive model (MAP-AR) is useful to correct a burst of length 70 symbols or less and any random errors when the transmission errors occur in a perpendicular magnetic recording channel. The proposed MAP-AR decoding outperforms the conventional MAP decoding in the BER performance of PR2 channel with these compound errors and gives reliable BER performance if the maximum burst error of length is shorter than the length of a column vector for the parity matrix of the array code.

Tue3-2 : Public Key Cryptography

Efficient Multiple Encryption from OW-PCA Primitives

Yang Cui, Kazukuni Kobara, Hideki Imai

Security of communication systems could be enhanced by multiple encryption (ME) has been noted by Shannon's pioneering work. Although this security for symmetric key encryptions was presented more than half a century ago, the appropriate one for public key encryptions has not been rigourously defined until very recently. However, it is common in ME that the total ciphertext will have a huge ciphertext overhead. This paper shows a general way to achieve this which could be proven to be the semantic secure multiple encryption, efficient from bandwidth viewpoint in particular.

A Simple Approach to Evaluate Fujisaki-Okamoto Conversion in Identity Based Encryption

Peng Yang, Takashi Kitagawa, Goichiro Hanaoka, Rui Zhang, Hajime Watanabe, Kanta Matsuura, Hideki Imai

The Fujisaki-Okamoto (FO) conversion is a very powerful security enhancement method in public key encryption (PKE) schemes. The generality of the plain FO in identity based encryption (IBE) schemes was verified, and a slightly different version, the modified FO, was proposed. Both of the plain FO and the modified FO could achieve the goal of converting a weak IBE scheme, i.e., one-way against adaptive chosen identity and chosen plaintext attacks (OW-ID-CPA), to the strongest one, namely, indistinguishability against adaptive chosen identity and adaptive chosen ciphertext attacks (IND-ID-CCA). This work aims to evaluate the plain FO and the modified FO by substituting proper concrete values. By mainly focusing on the time costs of security reductions, we show the modified FO is better than the plain one.

Notes on Several ID Based Cryptosystems

Ryuichi Sakai

The first collusion resistant executable ID based cryptosystems were proposed by Ohogishi-Sakai-Kasahara as the ID based key sharing scheme, and the collusion resistant ID based public key cryptosystems were proposed by them. Recently, Boneh-Byron and Waters propose ID based encryption schemes with security proofs in standard model. In this paper, we consider the structure of these schemes and modify the schemes. The main differences between modified version of the schemes and the original scheme is that the center knows the discrete log of the public parameter or not. We also show that if it makes that the original schemes can be always executed appropriately, the center must construct key parameter with the same orders of the modified schemes. In this case, the modified schemes can more freely select the key parameters compared with the original schemes. The efficiency of the encryption and the decryption of the modified schemes are same as the original schemes when in the original schemes the user pre-computes the pairing $\hat{e}(P_1, P_2)$.

A Public-Key Identification Scheme Based on a New Lattice Problem

Shunichi Hayashi, Mitsuru Tada

In this paper, we introduce a few decision problems related to lattices. These problems are shown to be NP-complete under many-to-one reductions. Moreover, we propose a public-key identification scheme based on one of these problems, and prove the security of the scheme. We also compare the efficiency of the proposed scheme to that of other identification schemes. The proposed scheme is more efficient than schemes based on NP-complete problems or lattice problems in round complexity. The scheme is also more efficient than schemes based on the discrete logarithm problem in asymptotical time complexity.

An Efficient N-Party Password-based Authenticated Key Exchange Protocol

SeongHan Shin, Kazukuni Kobara, Hideki Imai

In this paper, we propose an efficient N-party password-based authenticated key exchange (called N-PAKE) protocol where N clients who are sharing pair-wise passwords with a server want to establish a common session key securely. The N-PAKE protocol provides AKE-security and key privacy with respect to the server. In addition, the N-PAKE protocol is remarkably efficient rather than the previous works and each client's computational cost is independent with the group size. Specifically, each client involved in the protocol is required only four exponentiations and some negligible operations.

Tue3-3 : Multi-User Information Theory

Optimal Resource Allocation for a Bidirectional Regenerative Half-duplex Relaying

Tobias J. Oechtering, Holger Boche

In this work, we analyze the combinatorial structure of the achievable rate region of a spectral efficient bidirectional relaying decode-and-forward protocol, which makes future studies on the achievable stability region possible. Based on the insights on the combinatorial structure of this Gaussian channel further results on minimal necessary relay power and the maximal achievable sum-rate are derived. Finally, the scenario is extended by additional relay communication, where it is optimal to decode the relay message first. Furthermore, we derive the maximal possible relay rate for a given bidirectional sum-rate.

Characterization of Optimal Resource Assignments in the Framework of Blocking System Theory

Marcin Wiczanowski, Holger Boche, Slawomir Stanczak

We address the general problem of optimal orthogonal assignment of resources in a wireless network, e.g. in the form of assignment of carriers to links in a multi-carrier uplink/ downlink. We provide a step towards a better understanding of the assignment problem by a novel characterization of the optimizers and optimal values within the framework of blocking systems.

Characterization of the Fairness Gap in Resource Allocation for Wireless Cellular Networks

Holger Boche, Marcin Wiczanowski, Slawomir Stanczak

We address the relations between the notions of min-max fairness and max-min fairness in wireless cellular networks. We prove the existence of a performance gap between these fairness notions in general. We characterize network classes for which both fairness notions coincide and for which there exist power allocations which are fair in terms of both definitions.

On the Transport Capacity of Wireless Ad-hoc Networks

Sae-Young Chung

We show how transport capacity in bit-meters/s/Hz scales as the node density increases in ad-hoc networks. This was considered by many including. In this paper, we do not consider the scaling law of the transport capacity of the entire network, but focus on the transport capacity of one source-destination pair. We assume opportunistic routing is used to select the best relay node that is closest to the destination among nodes who successfully decode the current packet. We assume the squared channel gain decays as $e^{-\alpha d}/d^{\gamma}$, where $\alpha \geq 0$ is the absorption constant, $\gamma \geq 0$ is the path exponent, and d is the distance between a transmitter-receiver pair. We assume uniformly distributed nodes in n dimensions.

We show the transport capacity is bounded from above if there is no fading. Assuming slow flat Rayleigh fading and $\alpha = 0$, we show the transport capacity scales as $\Theta((\ln \lambda)^{1/\gamma})$ as the node density λ tends to infinity for one-dimensional networks. For any dimensional network, the transport capacity scales as $\Theta(\sqrt{\ln \lambda})$ if $\alpha = 0$ and $\gamma = 2$.

An Algebra for Log-Convex Interference Functions

Holger Boche, Martin Schubert, Marcin Wiczanowski

We study an interference-coupled multiuser network under the assumption of log-convex interference functions. Examples are interference models for matched-filter designs or channel uncertainties (robustness). We focus on the problem of maximizing the minimum signal-to-interference ratio of all users. We exploit that each log-convex interference function can be representeted as the product of basic building blocks depending on a non-negative stochastic coefficient matrix. For fixed coefficients, we provide necessary and sufficient conditions for the existence and uniqueness of a min-max optimal power allocation. Then, the results are generalized for arbitrary log-convex interference functions. The proposed theoretical framework provides a basis for the development and analysis of new resource allocation strategies based on log-convex models.

Tue3-4 : CDMA

A Non-Gaussian Coding Scheme that Exceeds Conjectured Gaussian Capacity Limit in CDMA Transmission with Single-User Decoding

Aminata Amadou Garba, Jan Bajcsy

Based on Gaussian signaling/interference arguments, it has been widely conjectured that the spectral efficiency limit on code-division multiple access (CDMA) transmission with single-user demodulation/decoding is about 0.72 bits per CDMA chip. Based on our recent channel capacity results for CDMA network transmission, we design a non-binary CDMA scheme that yields non-Gaussian multi-user interference and significantly exceeds the conjectured Gaussian capacity limit. In the proposed CDMA scheme, users' data are spread using a combination of time hopping, error-control coding and M-ary trellis coded modulation (TCM), i.e., no direct sequence spreading is employed. The receiver performs soft-decision single-user demodulation and iterative decoding between the TCM demodulator and the error correcting decoder. We present both designed TCM codes and simulation results for 16-ary and 64-ary CDMA transmission that achieve spectral efficiencies of 1.13 and 2.00 bits per chip, respectively.

CDMA Signal Design to Optimize Trade-off between the Bandwidth-efficiency and Power-efficiency in Uplink Systems

Atsurou Handa, Masahiro Fujii, Makoto Itami, Kohji Itoh

In this paper we compare two signal designs for uplink quasi-synchronous CDMA channels in order to optimize the trade-off between bandwidth-efficiency and power-efficiency. The one design, we call band-limited DS/CDMA design, is based on time domain assignment of Gold sequences just as in the ordinary DS/CDMA, with band-constrained cyclic chip interpolation functions, being unlike in the ordinary DS/CDMA. The other design, we call MC/CDMA design, is based on frequency domain assignment of the sequences as in MC/CDMA. The both designs presume insertion of guard intervals at the transmitter and frequency domain equalization in reception. Assuming quasi-synchronous arrival of CDMA signals at the

CDMA base station and FFT in the effective symbol interval, the inter-symbol interference is evaded in both designs. First we found the signal parameters which optimized the bandwidth-efficiency in band-limited DS design and MC design respectively. Second we found the signal parameters which optimize the power-efficiency in each of the designs. Finally we derived and compared the trade-off between the bandwidth-efficiency and power-efficiency of the band-limited DS and MC design. We found superiority of band-limited DS design to the MC design with respect to the optimized trade-off.

Localization of Radio-Controlled Car by Acoustic DS-CDM Signals

Shinji Tsuzuki, Naoyuki Takeichi, Yutaka Tano, Yoshio Yamada

The authors have proposed a beacon signal radiation system from the power-line for time synchronization among wireless and wired nodes. The considered application of the radiation system is an indoor fine-grained localization. Our rangefinder uses Direct-Sequence Code Division Multiplexed (DS-CDM) audible sound signals. This technique significantly improves performance in obstructed and noisy environments because of the diffraction of the sound wave and the spreading gain. In this paper, it is shown that the obtained average and worst accuracy of the localization in a $4m^2$ plane was 1cm and 4cm, respectively, under the ideal environment. The proposed method was also applied to find the location of a radio-controlled car. It is shown experimentally that although the localization accuracy was sensitive to the direction of the microphone, the average accuracy was less than 7cm in the $4m^2$ plane. As for the degradation due to the movement of the microphone, the allowed maximum speed, which avoid the effect of Doppler shift, was analyzed, and it was confirmed experimentally.

Keywords: Spread Spectrum Systems, Sensor network, Mobile node localization, Acoustic rangefinder, Doppler shift, Clock skew.

Generalized Random Spreading Performance Analysis of CDMA over GWSSUS Fading Channels

Özgür Ertuğ

Signal-to-interference ratio (SIR) experienced by users is the major quality and capacity indicator of CDMA systems. In this paper, we analyze the SIRs achievable with diversity-reception linear multiuser receivers over GWSSUS time-variant fading uplink DS-CDMA channels based on finite-dimensional generalized random spreading performance evaluation methodology. Through the results of random matrix theory on the non-asymptotic eigenvalue distributions of finite-size random matrices, SIR statistics with linear RAKE and decorrelating multiuser receivers are derived in terms of the key system parameters. Besides deciphering the performance expectations for finite-size systems independent of the specific choice and assignment of spreading sequences, the analysis of the derived average SIR expressions at the asymptotic wideband regime also further validate the predictions of previous large-system results on the deterministic SIRs with multiuser receivers at wideband limits.

Generalized MPSC and Its Performance in Synchronous Optical CDMA Systems

Tomoko K. Matsushima, Yasuaki Teramachi

A new class of codes for synchronous optical CDMA and a simple construction method of the codes are presented. The class, which is composed of codes constructed over extension fields GF(p^m), is a generalized version of the class of modified prime sequence codes (MPSCs), while original MPSCs are constructed over prime fields GF(p). It is shown that the proposed codes, which we call 'generalized MPSCs', have the same correlation properties with original MPSCs. Furthermore, this paper investigates the bit error rate performances of optical synchronous OOK and EWO systems employing interference cancellation techniques with generalized MPSCs. It has been shown that these systems can eliminate multiple user interference (MUI) errors completely, when they employ the original MPSCs. Our results show that the OOK and EWO systems employing generalized MPSCs also have the advantage to eliminate MUI errors.

Tue3-5 : MIMO (3)

A Practical Vector Dirty Paper Coding Scheme for MIMO Gaussian Broadcast Channels

Shih-Chun Lin, Hsuan-Jung Su

Recently, the vector dirty paper coding (DPC) achievable rate region has been shown to be the capacity region of a multiple-input multiple-output Gaussian broadcast channel (MIMO GBC). With DPC, the multiuser interference noncausally known at the transmitter can be completely removed. In this paper, we present a vector DPC structure for MIMO GBC channels. It is a generalization of the single antenna superposition coding for the scalar Gaussian dirty paper problem proposed by Bennatan et al. In a theoretical random code setting, this construction is shown to be able to achieve the promised rate performance of the MIMO GBC channel. We also implement it with existing vector quantizer and capacity-achieving channel coding. Combined with iterative decoding, an design example validates the effectiveness of our methods, which performs only 1.1 dB away from the capacity.

Approximate MLD for MIMO Systems Using Error Detection Scheme Based on LRAD

Dong-Jin Lee, Ryun-Woo Kim, Youn-Shik Byun

Maximum likelihood detection (MLD) for MIMO systems is known as an optimal method for signal detection in terms of bit error rate. However, the main drawback of MLD is its high complexity. To simplify the complexity of MLD, many linear and nonlinear techniques have been proposed. Here, we consider the lattice-reduction-aided detection (LRAD) scheme based on the well-known LLL algorithm for MIMO systems. By specific expression on rounding operation of LRAD scheme, we can search gap-symbols (error symbols) in the estimated symbols. As a result, performances of these methods approach more nearly to that of maximum likelihood detection that shows optimum performance. The complexities of these methods reduce and they converge on that of lattice-reduction-aided detection.

Code Controlled Sphere Decoding of Four Efficient MISO Lattices

Camilla Hollanti

Previously we have constructed some geometrically dense, full-rank, rate-one matrix lattices with large non-vanishing minimum determinants for 4 transmit antenna MISO applications. In this paper, we will consider the decoding of these lattices. The main concern is not in improving existing algorithms, but in finding a way to decode our lattices that are not as simple in structure, at least not at the first glance, as the majority of previously known ST lattices. We show that the decoding can be efficiently performed by using a modified version of a certain sphere decoding algorithm. We call this method "Code Controlled Sphere Decoding" (CCSD). Our lattice constructions are based on the theory of rings of algebraic integers and related subrings of the Hamiltonian quaternions. Simulations in a quasi-static Rayleigh fading channel have shown that our dense quaternionic constructions outperform the earlier rectangular lattices as well as the DAST-lattice.

A Consideration on the Complexity Reduction of LDPC Coded MIMO OFDM Receiver Structure

Le Khoa Nguyen, Yasunori Iwanami, Eiji Okamoto

Due to the increasing demands for the recent high capacity and high speed transmission in mobile communications, MIMO-OFDM (Multiple Input Multiple Output - Orthogonal Frequency Division Multiplex) schemes attract much attention. MIMO OFDM schemes are considered to be useful for Wireless LAN's, fourth-generation (4G) mobile phones, etc. On the other hand, LDPC (Low Density Parity Check) code seems to be an attractive channel coding scheme because of its very powerful error correction capability with less computational complexity. In the MIMO spatial multiplexing, the signal from

each transmit antenna must be separated. MLD (Maximum Likelihood Detection) can achieve the best BER performance, but it is pointed out that it needs the high computational complexity. To overcome this problem, we have investigated the QRM-MLD (Maximum Likelihood Detection with QR decomposition and the M-algorithm) and the SD (Sphere Decoding) w/o SQRD (Sorted QR Decomposition) in our proposed LDPC coded MIMO OFDM scheme. Furthermore, the soft output feedback from the LDPC decoder to the signal detector (SD, MLD, QRM-MLD), is used to generate the reliable soft replica, to extract the desired signal precisely from the spatially multiplexed signals.

Tue4-1 : Iterative Decoding

Reducing Computational Cost on Modified MDBF Decoding for High Dimensional Parity-Check Code

Yuuki Funahashi, Shogo Usami, Akira Ogawa, Ichi Takumi, Masayasu Hata

We have researched high dimensional parity-check (HDPC) codes that give good performance for channels over a very high error rate. HDPC codes are constructed using a combination of single parity-check codes, and it is easy to implement the code on hardware because of the simple structures. It can be said that HDPC codes are subset of LDPC codes. Maximum detected bit flipping (MDBF) decoding is known as a hard-in decoding method for HDPC codes with reasonable error performance and computational cost. We modified MDBF decoding for more improving error performance by introducing the parameter as decoding radius. However, modified method may make computational cost increase. In this paper, we propose an algorithm based on Modified MDBF(MMDBF) decoding to reduce computational costs with same error performance. The proposed method stops decoding when loop state is detected in decoding process. Then we perform computational costs to compare the proposed method with the original MMDBF decoding.

Reduced-Complexity Decoding of LDPC Codes Based on the Sum-Product Algorithm

Seho Myung, Kyeongcheol Yang

In this paper we propose a reduced-complexity algorithm for decoding LDPC codes. It is a simplified sum-product algorithm obtained by linearly approximating the function $\ln\cosh(x)$ and properly quantizing the received channel values. Simulation results show that the proposed algorithm does not cause a serious performance degradation, as compared with the floating-point sum-product algorithm.

On the Implementation of Belief Propagation (BP) Algorithm for Decoding Low-Density Parity-Check (LDPC) Codes

Young Seob Lee, Min Seok Oh, Jin Sung Choi

We present a simplified decoding algorithm reducing the complexity of BP algorithm with trivial performance loss. This algorithm is based on clever linear approximations of complex operations which usually would cause serious hardware complexity. For the approximation, existing decoding algorithms are discussed and a novel decoding processing is introduced in order to minimize performance degradation and hardware implementation cost. In addition, hardware architecture for the proposed algorithm is explained for the practical application of LDPC codes. In the simulation results, it is shown that the proposed algorithm produces almost same performance as the existing BP algorithm with signicantly reduced complexity.

On the Decoding of LDPC Codes in IEEE 802.16e Standards for Improving the Convergence Speed

Min-Ho Jang, Beomkyu Shin, Woo-Myoung Park, Jong-Seon No, In San Jeon

In this paper, the modified iterative decoding algorithm by partitioning check nodes is applied to low-density parity-check (LDPC) codes in IEEE 802.16e standards, which gives us the improvement for convergence speed of decoding. Also, the new method of check node partitioning which is suitable for decoding of the LDPC codes in IEEE 802.16e system is proposed. The improvement of convergence speed in decoding reduces the number of iterations and thus the computational complexity of the decoder. The decoding method by partitioning check nodes can be applied to the LDPC codes whose decoder cannot be implemented in the fully parallel processing.

Analysis of Complexity and Convergence Speed of Sequential Schedules for Decoding LDPC Codes

Sunghwan Kim, Min-Ho Jang, Jong-Seon No, Song-Nam Hong, Dong-Joon Shin

In this paper, a sequential message-passing decoding algorithm of low-density parity-check (LDPC) codes by partitioning check nodes is analyzed. This decoding algorithm shows better bit error rate (BER) performance than the conventional message-passing decoding algorithm, especially for the small number of iterations. Analytical results tell us that as the number of partitioned subsets of check nodes increases, the BER performance becomes better. We also derive the recursive equations for mean values of messages at check and variable nodes by using density evolution with Gaussian approximation. Finally, the analytical results are confirmed by the simulation results.

Tue4-2 : Data Network

Researches on Mobile Communications over a Private Address Area and a Global Address Area

Kazuto Enomoto, Hidekazu Suzuki, Junichi Sakamoto, Akira Watanabe

IP addresses are classified to two types of addresses, those are global addresses used in the Internet and the private addresses used only in the home networks or enterprise networks. In ubiquitous networks, it is desired that mobile terminals can move freely during communications without being conscious of difference of the address types. We have been proposed the technology called Mobile PPC which realizes mobile transparency. In this paper, we have researched the realization of mobile transparency over a private address area and a global address area by extending Moible PPC.

A Proposal of Voice over IP Passing through Firewall and Its Evaluation

Masashi Ito, Akira Watanabe

Due to development of communication infrastructure, IP telephone has reached a level of practice use. However, it is difficult to use IP telephone freely and safely, because there exist a firewall and a NAT between a global network and enterprise networks. In this paper, we propose a system called SoFW (SIP over Firewall) that enables passing through a firewall and a NAT by placing two relay agents on a global network and a private network, and generating an HTTP tunnel. Though there exist similar technologies, however, they need special terminals or integrated control of IP addresses. SoFW can use normal SIP terminals, and does not need integrated control of IP addresses, and it is easy to setup. We have implemented SoFW on Linux machines and confirmed the effectiveness.

Researches on Connections between WAPL and the Internet

Yoshiyuki Kato, Masashi Ito, Akira Watanabe

The technology of a mesh network attracts attention these days as the method of making wireless LAN easily. A mesh network makes it easy to set and maintain AP(Access Point)s in wireless LAN by connecting APs with an ad hoc network.In a mesh network, it is need to manage the information of relationships between the AP and terminals under the AP. We have been proposing WAPL(Wireless Access Point Link) as a mesh network. In this paper, principles of WAPL and its connecting method with the Internet are described.

Using Hybrid Method to Detect Internet Worms by Analyzing ICMP Type 3 Messages and Worm Characteristic Matching

WenHung Su, JaeHo Lee, Tomokazu Nagata, Shiro Tamaki

Recent well publicized attacks have made it clear that worms constitute a threat to Internet security. Internet worms can spread so fast that in-time human-mediated reaction is not possible. Therefore initial response to attacks has to be automated in early stage of worm spread. A useful method involves the use of ICMP Destination Unreachable (ICMP Type 3) messages generated from routers to detect the random scanning behavior of worms. But, as more and more people use peer to peer (P2P) file-sharing applications, using ICMP Type 3 messages to detect worm becomes difficult. The reason is that there are many similar activities between worm and P2P applications. But, by analyzing the worm activities, we still can get some characteristics only can be found in worms. In this paper, we present an early warning system by collecting and analyzing ICMP T3 messages and worm characteristic matching. By analyzing the ICMP T3 messages we can get doubtful events. By matching the characteristics of worms we can determine whether doubtful events are real worms or not. Therefore, we can detect a new worm in early infection stage and generate an alert to avoid serious damage.

An Error Control Scheme for the Routing Control Onboard the Satellite Repeater

Shunsuke Saiki, Akira Ogawa, Takaya Yamazato

This paper is concerned with performance evaluation for error control of the routing information onboard the simplified satellite repeater for broadband satellite communications. The necessary information for the onboard routing is carried on the preamble portion placed at the top of the packet and modulated with the differential binary PSK. In this paper, we adopt a simple two- dimensional parity check code for the routing information. It is decoded by iterated soft decision decoding, then the error correction is performed together with the erasure processing. We describe the results obtained by computer simulation in terms of the block error rate, the erasure rate and the erroneous erasure rate.

Tue4-3 : Network Coding

Characterization of Communication Cost Using an Information Theoretic Approach

Terence H. Chan

In this paper, we use an information-theoretic approach to study the minimal communication cost required to solve a distributive computing problem involving multiple participating parties connected by an underlying communication network. The set of admissible communication cost (in terms of the amount of information transmitted along each communication channel) tuples are identified and its outer bounds are also obtained. Furthermore, we prove that the separation of "data transportation" and "computation" layers may be suboptimal.

Architecture for Efficiently Decodable Network Codes

Terence H. Chan

This paper studies the use of "hypertrees" to disseminate data to a group of receivers. Compared to traditional routing-based approach, the proposed one can achieve higher network throughput (and hence can operate at a lower cost) at the expense of moderate increase in computing costs at receivers and a set of selected network nodes. A heuristic algorithm is then proposed to obtain cost-efficient hypertree-based multicast schemes.

Calculus of Service Guarantees for Network Coding

Ali Mahmino, Jérôme Lacan, Christian Fraboul

A large class of networks is able to provide some guarantees in terms of quality of service, end-to-end delays and throughput to data flows. In return, the data flows must verify constraints of burstiness and throughput.

The aim of this work is to introduce and evaluate the network coding for independent flows in such networks. First, we present efficient coding nodes strategies allowing the building of output flows as a combination of a subset of all the input flows. These strategies are evaluated in terms of maximal output throughput, maximum buffer size and maximal crossing-delays of the network node.

In a second part, we show that a generalization of these results to a complete network can be obtained through a transfer matrix whose entries are expressed in terms of network calculus.

Thanks to the formalism used to characterize the flows, the obtained results can be considered as guarantees in terms of the burstiness, buffers size or end-to-end delays.

Tue4-4 : Mobile Communications

A Consideration for Protection Ratio of Radio Relay System with Diversity Techniques for Frequency Coordination

Kyoung-Whoan Suh, Joohwan Lee

In this paper, the efficient and generalized algorithm of the protection ratio and its mathematical formulation are newly suggested for radio relay systems with diversity. The net filter discrimination has been also examined to see the effect of the adjacent channel protection ratio caused by adjacent channel interference. Protection ratios are investigated in terms of diversity improvement factor related with main and diversity antenna gains, distance between main and diversity antennas, and carrier frequency. The presented method gives easy and systematic extension to calculate the protection ratio and can be applied to the initial planning of frequency coordination for fixed wireless networks up to millimeter wave band.

An Improvement of Closed-loop Transmit Diversity with Three Transmit Antennas

Manabu Sugawara, Eiji Okamoto, Yasunori Iwanami

Transmit diversity techniques is one of the solutions in the wireless communication. In this techniques, multiple antennas are used in the transmitter, and it enables a small and lightweight receiver. Moreover, transmit diversity needs feedback bits, including the information of fading in the channel from receiver to transmitter, because the fading needs to be equalized at the transmitter. The feedback information is quantized at the receiver to reduce the number of bits. In the quantization, the information vector is quantized into a fixed point or a differential phase, and it is known that the iterative LIoyd algorithm is effective in this calculation. In this paper, we propose an improvement scheme of closed-loop transmit diversity which generates a better performance with fewer feedback bits based on LIoyd algorithm.

A Study on Route Diversity Effect Using Turbo Codes in Mesh Networks

Tadahiro Wada, Abbas Jamalipour

In this paper, we show the performance of route diversity effect in wireless mesh networks. Wireless mesh networks are a key technology for next generation wireless networking. In the mesh networks, many relay nodes are spread in a geographical area and make an ad-hoc wireless network having a mesh structure. Multi-route transmissions are available in the mesh networks and can achieve high link quality because of the route diversity effect. It is well known that forward error correction schemes and turbo codes significantly enhance the diversity effect. In this paper, we investigate the route diversity effect by turbo codes in wireless mesh networks. We evaluate the BER performance in the mesh networks and show that the effect can prevent large performance degradation against AWGN environment.

Analysis of Jong Nang Multiple Access Channel

MoonHo Lee, Xueqin Jiang, Chang-hui Choe, Sung Hoon Kim

In this paper, we describe the Jong Nang which used the binary system similar to digital communications and computers today. Three timbers were exactly like three binary digits. And we compute the capacity of the Jong Nang channel, and propose a modified code for the Jong Nang detect the error in case that at an error occurs because one timber falls down from its place.

A Simple Cooperative Mobile Selection in Cooperative Diversity System

Sung-Yeon Kim, Hyo-Shil Kim, Youn-Shik Byun

Cooperative diversity has been recently proposed as a way to form virtual antenna arrays that provide dramatic gains in slow fading wireless environments. However, most of the proposed solutions require distributed space-time coding algorithms, the careful design of which is left for future investigation if there is more than one cooperative relay. We propose a simple cooperative mobile selection in cooperative diversity system. The power and the bandwidth of the proposed cooperative user selection scheme are equal to those of a cooperative and non-cooperative scheme. By using this method, transmitted signals are sent to multiple users, and then to the base station. The performance of cooperative diversity is best when select maximizing channel capacity among branch channel capacities. The success (or failure) to select the best available path depends on the statistics of the wireless channel, and a methodology to evaluate performance for any kind of wireless channel statistics, is provided. Information theoretic analysis of outage probability shows that our scheme achieves the same diversity-multiplexing tradeoff as achieved by more complex protocols, where coordination and distributed space-time coding for relay nodes is required, such as those proposed by Laneman and Wornell (2003). The simplicity of the technique allows for immediate implementation in existing radio hardware and its adoption could provide for improved flexibility, reliability, and efficiency in future 4G wireless systems.

Tue4-5 : OFDM

New Selection Method of Near Optimal PRT Set in TR Scheme for PAPR Reduction of OFDM

Dae-Woon Lim, Hyung-Suk Noh, Jong-Seon No, Dong-Joon Shin

In the tone reservation (TR) scheme, it is known that the set of randomly selected peak reduction tones (PRT's) performs better than the contiguous PRT set and the interleaved PRT set in the PAPR reduction of orthogonal frequency division multiplexing (OFDM). It is also known that finding the optimal PRT set corresponds to the secondary peak minimization problem in the TR scheme. But, the problem cannot be solved for the practical number of tones since it is NP-hard. In this paper, a new search algorithm for the near optimal PRT set is proposed based on the fact that the secondary peak value of the PRT set statistically tends to decrease as the variance of the PRT set decreases.

Frequency Domain Turbo Equalization Combined with Frequency Offset Compensation in Uplink OFDMA Systems

Yuusuke Miyauchi, Takahiko Saba

In uplink orthogonal frequency division multiple access (OFDMA) systems, the amounts of carrier frequency offset (CFO) are different in each user. CFO spoils the orthogonality among subcarriers, and causes intercarrier interference (ICI) and multiple access interference (MAI). Since ICI and MAI degrade the demodulation performance significantly, CFO compensation is required in uplink OFDMA systems. In this paper, we propose a CFO compensation scheme which uses frequency domain turbo equalization with soft cancellation. The proposed receiver accomplishes CFO compensation and channel equalization simultaneously in the frequency domain. Simulation results show that the proposed receiver attains a bit error rate (BER) performance which is almost the same as that in the case without CFO when the variance of offset among users is small.

Turbo Detector Using Modified SISO-MLD for CCI Suppression in LDPC Coded SDM-OFDM Systems

Shoichi Sasahara, Takahiko Saba

In space division multiplexing with orthogonal division multiplexing (SDM–OFDM) systems, since co-channel interference (CCI) degrades the demodulation performance, CCI suppression is essential. For CCI suppression, a turbo detector with soft cancellation (SC) followed by minimum mean square error (MMSE) filter is well known. However, although SC/MMSE detector realizes the turbo detection by simple processing, it requires a number of iterations to achieve a reasonable CCI suppression performance. Therefore, we consider to apply maximum likelihood detector (MLD) to the turbo detector. In this paper, we propose an SC/MLD to improve the CCI suppression performance in LDPC coded SDM–OFDM systems. In our proposed detector, soft-in soft-out (SISO) MLD is employed and modified to cope with SDM–OFDM systems. From the simulation results, the performance of SC/MLD is superior to that of SC/MMSE detector by more than 3 [dB] of bit error rate (BER) of 10^{-3}.

Reactance-domain Modulation Scheme for Burst Error Reduction of ISDB-T in Slow Fading Environment

Young-Cheol Yu, Minoru Okada, Heiichi Yamamoto

In this paper, we propose a reactance-domain modulation scheme for burst error reduction of ISDB-T (Integrated Services Digital Broadcasting for terrestrial) in slow fading environment. The Japanese DTTB (Digital Terrestrial Television Broadcasting) standard, ISDB-T, employ OFDM (Orthogonal Frequency Division Multiplexing) for its transmission scheme. Thanks to the efficient FEC (Forward Error Correction) with long-depth time interleaving, ISDB-T is capable of receiving the signal in severe fading channel. In slow fading environment, burst error deteriorates its performance because the fade duration exceeds the interleaving depth. In order to solve this problem, we propose a reactance domain modulation scheme, which virtually generates the fast fading for efficient use of time interleaving. Our proposed scheme can solve burst error problem in slow fading environment. Computer simulation results show effectiveness of our proposed scheme.

Delay and Buffer Size Bounds for OFDM Broadcast Systems

Gerhard Wunder, Chan Zhou, Thomas Michel

Upper bounds on the maximum average delay and queue length of an OFDM broadcast system are derived. The system is modeled as a queue system including information-theoretic and queuing-theoretic characteristics like the channel state, the power constraint and packet arrival rate. Choosing an appropriate set of Lyapunov functions a general path for bounding the polynomial moments is provided. Explicit bounds are provided for the first and second moment. Furthermore, it is shown that all moments are finite and converge geometrically to their stationary values. Thus, the system is stable in a very strong sense.

Wed1-1 : Weight Distribution

Asymptotic Average Coset Weight Distribution of Multi-Edge Type LDPC Code Ensembles

Kenta Kasai, Yuji Shimoyama, Tomoharu Shibuya, Kohichi Sakaniwa

Multi-Edge type Low-Density Parity-Check codes (MET-LDPC codes) introduced by Richardson and Urbanke are generalized LDPC codes which can be seen being constituted of some standard (ir)regular LDPC codes. We prove MET-LDPC code ensembles possess a certain symmetry with respect to their average coset weight distributions (ACWD). Using the symmetry, we drive asymptotic ACWD of MET-LDPC code

ensembles from asymptotic ACWD of their constituent constituent ensembles.

Support Weight Distribution of Regular LDPC Code Ensembles

Takayuki Itsui, Kenta Kasai, Ryoji Ikegaya, Tomoharu Shibuya, Kohichi Sakaniwa

The support weight distribution of a code is the number of subspaces of the code with specified dimension and support weight. In this paper, we formulate the average support weight distribution of regular LDPC code ensembles.

New Probabilistic Algorithm to Enhance the Reliability of Computed Weight Distribution of LDPC Codes

Masanori Hirotomo, Masami Mohri, Masakatu Morii

We have proposed a probabilistic method for computing the weight distribution of LDPC codes. In this method, we use Stern's algorithm which finds the low-weight codewords to estimate the weight distribution for the low-weight codewords. However, there are some differences between the computed weight distribution and the true weight distribution. In this paper, we propose two probabilistic algorithms in order to estimate the weight distribution of LDPC codes with high accuracy. These algorithms are used instead of Stern's algorithm to find the low-weight codewords quite randomly. Using these algorithms, we can improve the reliability of the weight distribution computed by the probabilistic method.

An Efficient Method for Computing the Minimum Weight of High Rate Binary Cyclic Codes

Zheyu Li, Masami Mohri, Masakatu Morii

It is important to develop the efficient method for computing the minimum weight of error correcting codes in order to estimate the performance of the codes. In general, it is difficult to compute the minimum weight d_{min} or the number of codewords with its weight for the (n, k) linear code with large codelength n and information digits k. Although some efficient methods for binary cyclic codes with low rate have been proposed, efficient method has not shown for the code of high rate. In this paper, we propose a method for computing the minimum weight of binary (n, k) cyclic codes with high rate $(k/n > 1/2)$. It is based on the properties of *n-sparse*. For any binary (n, k) cyclic codes with high rate, the complexity of our method is very small compared with the conventional methods.

On Relation between the Defining Set and the Weight Distribution for Cyclic Codes

Takayasu Kaida, Junru Zheng

We discuss the weight distribution for cyclic codes defined by the defining sets. In order to study on relation between the defining set and the weight distribution, a condition for connecting with cyclic codes by distinct defining sets is investigated. Moreover some examples of binary cyclic codes with length 15 and 63 are given.

Wed1-2 : Quantum Information Processing (1)

Property of Optimum Quantum Detection for Mixed States with Non Gaussian and Gaussian Noise

Toshiyuki Tsuchimoto, Tomohiro Sawada, Shogo Usami, Tsuyoshi Sasaki Usuda, Ichi Takumi

To derive an optimum detection minimizing the average probability of error is a fundamental problem in quantum detection theory. So far, optimum detections have been derived for many signals. Almost solutions are for pure-state signals. However, a study of mixed-state signals is important not only for reliable communications but also for secure communications. In the present paper, a property of minimum error probability is considered for mixed states with non Gaussian noise, which are artificial mixed-state signals.

Characteristics of Classical Capacity of an Attenuated Channel Assisted by Orthogonal Entangled States

Seiji Hattori, Tsuyoshi Sasaki Usuda

It had been shown that use of entanglement enhances classical communications. We compute the capacity $C_{\mathrm{Bell}}^{(1)}$ assisted by orthogonal entangled states. We compare it with the capacity C_{sq} assisted by two-mode squeezed states when the quantum channel is an ideal channel or an attenuated channel.

Counter-examples of the Trace Inequalities Related to the Auxiliary Function of the Quantum Reliability Function

Shigeru Furuichi, Kenjiro Yanagi

We study the open problem given by Holevo and Ogawa-Nagaoka on the concavity of the auxiliary function of the quantum reliability function. Firstly we review the previous results on this problem in the case that the parameter s is positive. Secondly we consider the problem in the case that the parameter s is negative.

Artificial but Fully Quantum Description Approach to Quantum State Distinction Problem

Kentaro Imafuku, Hideki Imai

When distinguisher, who tries to distinguish two non-orthogonal quantum states, employs the best strategy, the interference term between the "success world" and "failing world" vanishes.

Wed1-3 : Random Number

Generation of a Discrete Distribution Using Biased Coins

Danielle P. B. de A. Camara, Valdemar C. da Rocha Jr., Cecilio Pimentel

The efficient generation of a discrete probability distribution is of current interest in areas like cryptography and random number generation. This paper presents an algorithm for generating a discrete distribution using two or more coins, being one of them unbiased. In particular, this approach contributes an alternative solution to the classical problem of generating a discrete uniform probability distribution using two or more distinct coins.

Analysis for Pseudorandom Number Generators Using Logistic Map

Shunsuke Araki, Takeru Miyazaki, Satoshi Uehara

We are studying a pseudorandom number generator with the logistic map. A suitable basic parameter, a precision of the generator, must be needed in order to design an algorithm of the generator. In this paper we defined a simple algorithm of the generator and checked randomness for the output by the NIST statistical test. Thus this numerical experiment shows the shortest precision, 56 bits. Additionally, we discussed why two precisions, 54 bits and 60 bits, were not suitable parameters. Last, we gave an attack for the generator with a short precision.

Correction of Overlapping Template Matching Test Included in NIST Randomness Test Suite

Kenji Hamano, Toshinobu Kaneko

Accurate values for occurrence probabilities of the template used in the overlapping template matching test included in NIST randomness test suite (NIST SP800-22) have been analyzed. The inaccurate values used in the NIST randomness test suite cause significant difference of pass rate. When the inaccurate values are used and significance level is set to 1%,

the experimental mean value of pass rate, which is calculated by use of random number sequences taken from DES (Data Encryption Standard), is about 98.8%. In contrast, our new values derived from a set of recurrence formulas for the NIST randomness test suite give an empirical distribution of pass rate that meets the theoretical binomial distribution. Here, the experimental mean value of pass rate is about 99%, which corresponds to the significance level 1%.

A Keystream Resynchronization by Time and Precision Information

Janghong Yoon

An Effective Simple Fuzzy Approach for Stable Real Random Number Generator

Sunchun Park, Youngmi Park, Daesun Park, Chunsu Kim, ChoogHo Cho

Wed1-4 : Sensor Networks

Measurement of Distance Between Nodes in an Ad-hoc Network by Multiple Acoustic Waves

Wataru Uemura, Masashi Murata

On ad-hoc network, distance information between nodes is needed for making packets routing tables. Usually we get information of a wireless signal power from a wireless network card because there is a relationship between the wireless signal power and distance information between nodes. Some network cards, however, do not provide us a wireless signal power or such information. In this paper, we provide a novel distance measurement method using acoustic waves. The receiving acoustic waves consist of a direct wave and reflected waves. The power of the direct wave varies inversely as the distance, and the power of the reflected waves have periodicity. It is too difficult for a node to know the distance information from the power of the receiving acoustic wave because of the periodicity of reflected waves. The periodicity of reflected waves depends on the wave length. In this paper, we propose the distance measurement method with multiple sine waves. And experiments show its implementability.

Acoustic Sensing for Detection of Approaching Vehicles

Kensaku Asahi, Fumiyasu Miyoshi, Akira Ogawa

We have been in research for preventing vehicles from head-on collision by sound, and focused on the sound from tires of a vehicle. So far, the direction of approaching vehicles has been detected with two microphones onboard the vehicle, which is called the basic scheme. The detection time of the basic scheme, however, may be affected by ambient noise such as sound of engine. We have developed an improved scheme in which the direction of approaching vehicle is to be detected from the sound signals captured with multiple pairs of microphone arrays. In addition, experimental results on the effect of engine sound are shown in this paper.

Bayes Stopping Rule for Wireless Sensor Networks

Jin Kyung Park, Woo Cheol Shin, Jun Ha, Cheon Won Choi

A wireless sensor network is a network of compact microsensors equipped with wireless communication capability. In a wireless sensor network, sensor nodes are usually battery-powered and it is difficult to change or recharge their batteries. Also, a wireless sensor network is often deployed to collect and update data periodically. Late delivery of a data segment by a sensor node causes the sink node to defer data processing and the data segment itself to be obsolete. Thus, such a wireless sensor network gives rise to two critical issues; saving energy and supporting timeliness in data delivery. Intending to resolve these issues, we propose a version of ALOHA as a MAC scheme for a wireless sensor network. While conserving the simplicity and robustness of the original version of ALOHA, the proposed version of ALOHA possesses a distinctive feature that a sensor node decides between stop and continuation prior to each delivery attempt for a packet. Such a decision needs a stopping rule and we suggest a Bayes stopping rule. Note that a Bayes stopping rule minimizes the Bayes risk which reflects the energy, timeliness and throughput losses. Also, a Bayes stopping rule is practical since a sensor node makes a decision only using its own history of delivery attempt results and the prior information about the failure in delivery attempt. Numerical examples confirm that the proposed version of ALOHA combined with a Bayes stopping rule is a useful MAC scheme in the severe environment of wireless sensor network.

Iterative Joint Channel-Decoding Scheme Using the Correlation of Transmitted Information Sequences in Sensor Networks

Kentaro Kobayashi, Takaya Yamazato, Hiraku Okada, Masaaki Katayama

In this study, we consider joint channel decoding of Turbo code for multiple correlated data that are observed by sensor nodes densely deployed in a sensor field. We focus on the correlation properties of observation data and try to reduce decoding error by an iterative procedure. An approach to use practical channel codes for more than two correlated data is still not presented. A problem in the extension to cases of more than two sensor nodes is how to use the information of correlation obtained from observation data. In this study, we propose an iterative channel decoding scheme that uses them with weighting. We show that when the number of sensor nodes is increased, decoding performance improvement cannot be achieved by simple weighting, and so a more appropriate weight is needed. We find the optimum weight that minimizes the bit error rate from the analytical formula for uncoded BPSK and apply it to the case of Turbo code.

Wed1-5 : Image & Speech

Sign-only Synthesis

Zhimei Yang, Hiroshi Kondo, Takaharu Koda, Lifeng Zhang

Sign-only syntheses [1] of several typical and real orthogonal transforms are presented. Phase-only synthesis is introduced by "Image recovery -Theory and Application-" written by Henry Stark. Sign-only synthesis is the extended version of the Phase-only synthesis. Sign-only synthesis is defined as an inverse transform of only signs of the transform coefficients and has a variety of applications. Employed orthogonal transforms are Discrete Cosine Transform, Hadamard transform, Binarized Fourier Transform and Karhunen-Loeve Transform. These transforms have real number resulting coefficients and then it looks interesting to know the property of each transform signs. The characteristics of these Sign-only synthesis are compared each other. And interesting nature of transform signs are extended. One application of Sign-only synthesis is shown as a facial authentication. Keywords : Orthogonal transforms, Sign-only synthesis , Discrete Cosine Transform, Hadamard Transform , Binarized Fourier Transform, Karhunen-Loeve Transform

Statistical Methods for a Large Vocabulary Continuous Speech Recognition System for Hindi

Kshitij Gupta, Pramod Kumar Sharma

In this paper we describe a large vocabulary continuous speech recognition (LVCSR) system for Hindi based on statistical methods. While a rule based approach provides a reasonable spelling to phone sequence mapping, it, however, requires an in-depth knowledge of the linguistics of the language and becomes difficult to account for certain anomalies through rules. Statistical methods provide a better alternative by using the training data available to develop trainable models that adapt to actual speech with greater ease and efficiency as compared to the rule based techniques. Hidden Markov Models (HMM) have been utilised for modelling continuous speech, with phone sized segments and Gaussian Mixture Models (GMM) for modelling probabilities which also facilitate associating acoustic differences with corresponding labels. We present a complete overview of the proposed system from the initial speech signal processing using Mel filter cepstral coefficients (MFCC), through acoustic modelling using HMM that incorporates ini-

tialisation as well as training, and the language model, finally elaborating upon the Viterbi decoding for recognition. Special emphasis has been laid on aspects of the system that are language specific and should be adapted for better output.

Supplement to a Theorem for Biorthogonal Bases of Wavelets and a Consideration of Four-term Sequence (h_n)

Hajime Sato

We propose a variation of the theorem already obtained in 1992 by Cohen, Daubechies and Feauveau to give necessary and sufficient conditions for biorthogonality of the corresponding scaling functions ϕ and $\widetilde{\phi}$. Their theorem brings us a simple procedure to check that a pair of *finite* real sequences (h_n) and $(\widetilde{h}_n)$ generate biorthogonal bases of wavelets.

We make a single-sequence version of the theorem to give necessary and sufficient conditions only for (h_n) to generate a scaling function ϕ of some multiresolution analysis. Since for any scaling function ϕ there exists at least one scaling function $\widetilde{\phi}$ with biorthogonality to each other, our conditions turn out to be sufficient for (h_n) to generate biorthogonal wavelets. The associated sequence $(\widetilde{h}_n)$ is not necessarily finite, in this case.

Numerical results about 4-term sequences (h_n) satisfying our conditions are depicted.

Application of Background Subtraction with Renewable Background to Gesture Region Extraction

Akio Ogihara, Hiroshi Matsumoto, Akira Shiozaki

Background subtraction algorithm is often used in image processing in order to extract moving object. In this paper, we propose a new background subtraction algorithm. In the proposed method, we introduce the renewal of background image according to the situation of input image. In comparison with the conventional method, our method is able to extract moving object more accurately and more efficiently. Moreover, the proposed method has been applied to gesture region extraction as one of its applications.

A Study on the Expansion of a Resolution Conversion Method into Rational Scale Using Neighboring Blocks' DCT Coefficients

Tomio Goto, Yoshihiro Shinkai, Masaru Sakurai, Tadashi Kitamura

There are a number of approaches for converting image resolution. In general, resolution conversion takes place in the spatial domain, which is a straightforward method. However, DCT (Discrete Cosine Transform) is often used in image compression. Resolution conversion in the DCT domain is noteworthy because this method can convert image resolution with compressed image data (ex. JPEG and MPEG formats) without decoding so that the resolution conversion process in this method is faster than that in the straightforward method. However, there are many problems in which the scaled up images have blocky noise, the edges are blurry and the basis length after transformation is not the same as before transformation, so general decoders such as JPEG and MPEG cannot be used in this method.

We have proposed a new conversion method in the DCT domain using neighboring blocks' DCT coefficients. It is possible to convert image resolution and to improve resolution conversion images by decreasing edge blur and blocky noise. However, using this method was not possible to scale up at rational rates, and it was not useful for resolution conversion. So, we propose an expansion to rational rates for this method.

Wed2-1 : Coded Modulation and Space-Time Codes

Improved Decoding for Trellis Coded Modulation with a Convolutional Processor

Yeong-Luh Ueng, Ruey-Yi Wei, Chia-Jung Yeh, Mao-Chao Lin, Jun-Yun Lu

It is already known that trellis coded modulation (TCM), constructed by using the encoder of a convolutional code C with short constraint length followed by a convolutional processor and a signal mapper, can achieve large squared free distances, where the convolutional processor is a rate-one convolutional code with large constraint length. The previously used decoding results in large error coefficients and hence the obtained coding gain is distant from the asymptotic coding gain. In this paper, we propose to use an expanded trellis of C with some recovered information to decode the TCM. With the proposed decoding, additional coding gain can be obtained as compared to the previously used decoding.

Golden Space-Time Trellis Coded Modulation

Yi Hong, Emanuele Viterbo, Jean-Claude Belfiore

In this paper, we present a multidimensional trellis coded modulation scheme for a high rate 2×2 multiple-input multiple-output (MIMO) system over slow fading channels. Set partitioning of the Golden code is designed specifically to increase the minimum determinant. The branches of the outer trellis code are labeled with these partitions. Viterbi algorithm is applied for trellis decoding. In order to compute the branch metrics a sphere decoder is used. The general framework for code optimization is given. Performance of the proposed scheme is evaluated by simulation and it is shown that it achieves significant performance gains over uncoded Golden code.

New Optimal Rate-Diversity Tradeoff Space-Time Codes with Adaptive Iterative Decoding

Wen-Hsien Chiu, Hsuan-Jung Su

The design of smart-greedy space-time (ST) codes for multiple-input multiple-output (MIMO) wireless systems in a variety of mobility conditions is an open problem of great interest. Motivated by the space-time codes proposed by Lu and Kumar, which achieve the optimal tradeoff between the transmission rate and the transmit diversity gain, we propose an algebraic method for constructing optimal rate-diversity tradeoff ST codes in the smart-greedy sense. This construction is shown to achieve the optimal rate-diversity tradeoff in quasi-static fading channels and provide outstanding potential for seizing temporal diversity in fast fading channels.

Performance Comparison Between Conventional Space-Time Block Code and Proposed Constellation Rotation Space-Time Codes

Mea-Hwa Park, Hyo-Shil Kim, Jong-Deuk Kim, Youn-Shik Byun

Conventional STBC(Space-Time Block Code) from orthogonal designs proposed by Alamouti [1], have attracted much attention lately due to their fast MLD(Maximum Likelihood Decoding) and full diversity. But coding gain is another important factor in the performance of the system. Face to this problem, we analyze the performance of multiple transmit/receive antenna systems with CR(constellation Rotation) precoder called CR-STC. STBC which based on CR code has maximum diversity gain and more coding gain than conventional STBC without sacrificing additive bandwidth in frequency quasi-static fading channels. In this paper, we set the receive antenna number 2, and combine the improved STBC which based on new CR codes with MIMO-OFDM systems. Then continue to analyze the performance of system with the schemes proposed in this paper. Finally, we make a comparison between the performance of the system with new proposed CR-ST algorithms and that of conventional scheme. Using 4QAM modulation, simulation result shows the proposed scheme called *Method* 1 and *Method* 2 have about 0.5 dB, 1 dB more performance improvements than conventional STBC at BER=10^{-2}, respectively.

Wed2-2 : Quantum Information Processing (2)

Entanglement of Formation of a Decohered Quasi-Bell State

Ryutaro Yamamoto, Tsuyoshi Sasaki Usuda, Ichi Takumi

Recently it has been shown that the entangled state by nonorthogonal states such as coherent state of light can have complete degree of entanglement. However, when we generate it experimentally and apply to quantum protocols, it is necessary to consider various incompleteness of the entangled states. In the present paper, we consider degradation property of entanglement of decohered quasi-Bell states by using Entanglement of Formation.

Quantum Secure Direct Communication Protocols for Sending a Quantum State

Yumiko Murakami, Masaki Nakanishi, Manabu Hagiwara, Shigeru Yamashita, Yasuhiko Nakashima

We propose a new quantum secure direct communication protocol, which has an advantage of combining the following features over related works: The protocol allows us to send a quantum state in security; The proper sender and receiver can detect an eavesdropper efficiently; The protocol employs no entanglement resource, and thus it is relatively easy to be experimented in current technology.

Uncertainty Principle and Oblivious Transfer

Takayuki Miyadera, Hideki Imai

We discuss security of a quantum protocol by using the uncertainty relation, the most fundamental principle of the quantum theory. We generalize a "probabilistic" uncertainty relation which was obtained by I.Damgaard, S.Fehr, L.Salvail, and C.Schaffner to prove the security of quantum oblivious transfer under the assumption of quantum bounded storage. Our generalization yields us to generalize their result on the memory size to more realistic circumstance.

Perfect Single-Error-Correcting Binary Code for Interactive Secret Key Reconciliation

Koichi Yamazaki

How to construct perfect single-error-correction codes for interactive secret key reconciliation is proposed to reduce the process time of secret key reconciliation protocol, which could be dominated by interactive communication through public channel. First, we show the Hamming bound modified for error correcting codes for an interactive secret key reconciliation. Then we propose explicit coding and decoding algorithms. Parity check matrices proposed here is constructed by modifying binary Hamming codes. Computer simulation results are given to compare performance of an interactive secret key reconciliation with the proposed code and BBBSS protocol.

Wed2-3 : Pattern Recognition

A Note on Spelling Correction Methods Based upon Statistical Decision Theory

Yasunari Maeda, Hideki Yoshida, Yoshitaka Fujiwara, Toshiyasu Matsushima

A spelling correction problem is one of important topics in the field of NLP(Natural Language Processing). In previous research a DMC(Discrete Memoryless Channel) with unknown parameters has been used as a model for generating misspelled words. In the previous research the spelling correction problem was divided into two problems, estimating the unknown parameters of stochastic models and correcting misspelled words. MLE(Maximum Likelihood Estimate) was used in the previous research basically, but there was no reason why MLE was used. There was no theoretical guarantee when the number of data for learning was finite.

In this paper we treat estimating the unknown parameters and correcting misspelled words as one problem based upon statistical decision theory. In the spelling correction problem there are three kinds of error rates, an error rate per sentence, an error rate per word, an error rate per alphabet. The error rate is the probability of failure in correcting misspelling. In this paper we treat the error rate per sentence and the error rate per word. We propose optimal methods which minimize the error rates with reference to the Bayes criterion and approximate methods in order to reduce computational complexity.

Fast Nearest Neighbor Search Algorithm for Waveform Quantization Using Reflection Group

Shuichi Maki, Nobumoto Yamane, Yoshitaka Morikawa

Highspeed implementations have been studied in the field of vector quantization (VQ). In the existing prequantization (PQ) method, we fast quantize an input vector by scalar quantization (SQ) and then we perform full search (FS) VQ by using the reduced codebooks corresponding to SQ outputs(P-SQ). This paper, using kaleidoscope VQ (KVQ), extends the PQ method to VQ on unit hypersphere(P-KVQ). KVQ is considered as hyperspherical lattice VQ, in which lattice points can be generated by reflections, and can be implemented only by sorting and signchanging of input vector components. Computer simulations, using 4 and 8 dimensional codebooks designed for uniform hyperspherical distribution, showed that we can reduce quantization time to 3% of the direct FSVQ and superiority of P-KVQ for P-SQ is shown by comparisons of memory amount.

The Entropy Potential of a Discrete Probability Distribution

Jan Poland

In this paper, a new information theoretic quantity for a probability distribution $\{p_\nu : \nu \in \mathcal{N}\}$ on a discrete space $\mathcal{N}$ is studied: the *entropy potential*. It is defined as the maximal entropy of all of the following legal transformations of the distribution: There is one *reference element* $\mu \in \mathcal{N}$, and the respective probability p_μ is kept fixed. All other probabilities p_ν $(\nu \neq \mu)$ can be arbitrarily decreased, after which the distribution is renormalized. It is shown that the entropy potential is a natural quantity describing the uncertainty of a class of hypotheses where one hypothesis is true, e.g. in Bayesian learning. In particular, performance guarantees for a stochastic model selection learner can be shown using the entropy potential. We prove characterizations and estimates, and compute the entropy potential for broad classes of discrete probability distributions.

User Verification Method by Biometric Feature in Keystroke Motion and Key Press Timing

Akio Ogihara, Hiroyuki Matsumura, Akira Shiozaki

We propose an ATM (automatic teller machine) user verification method using biometric feature in keystroke motion. In the proposed method, ATM user verification is performed by using the 10 types of biometric feature which are extracted from hand-shape in ATM operation. Moreover, we calculate the similarity between current operator and genuine user in consideration of key-press timing. The proposed method can improve the safety of the present situation without special additional operation, physical load and psychological burden.

Wed2-4 : Ad Hoc Networks

Equalization Techniques for Multihop Cooperative Wireless Networks with Asynchronous Relaying

Ryu Yamashita, Hidekazu Murata, Susumu Yoshida, Kiyomichi Araki

This paper presents the performance of a cooperative relaying scheme using single carrier transmission with frequency domain equalization (SC-FDE) and that with time domain equalization (SC-TDE). A cooperative relaying scheme is the key technique for multihop wireless networks to improve its end-to-end transmission performance. When this network is an autonomous distributed network, timing synchronization

among relay stations in the hop is a challenging task since propagation delays are inevitably different among relay stations. In this paper, equalization techniques are employed to cope with time asynchronous received signals from the previous hop. A delay diversity technique is used as a transmit diversity scheme for cooperation, since an equalizer can be used not only to overcome asynchronous received signals but also to demodulate the signals with delay diversity. By computer simulations, the effects of delay diversity and asynchronous relays are investigated when SC-FDE and SC-TDE are applied to a cooperative relaying.

Adaptive Modulation Schemes for Multihop Cooperative Wireless Networks

Bao Thi Ngoc Pham, Hidekazu Murata, Susumu Yoshida, Kiyomichi Araki

Wireless multihop communications with cooperation of multiple relay terminals at each hop give diversity effect and show a significant frame error rate performance improvement than that without cooperation. To improve the spectral efficiency of this communication networks, adaptive modulation is considered.

In this paper, three schemes for adaptive modulation controls are investigated in cooperative multihop networks. Throughput performance of these schemes are investigated by computer simulations in Rayleigh fading channels assuming a delay diversity technique. In simulations, the received SNR is estimated based on the path metric of the Viterbi algorithm, and the channel estimation is done by recursive-least-squares algorithm (RLS).

Adaptive Node Selection Algorithm for Co-operative Multi-hop Networks

Ryu Atsuta, Takahiko Saba

In multi-hop networks, the quality of transmission in a lower signal to noise power ratio (SNR) link is improved by co-operative transmission. However, in a higher SNR link, co-operative transmission increases traffic load. Hence, the number of co-operation nodes (C-nodes) is cautiously determined when co-operative transmission is employed. In this paper, we propose an adaptive algorithm to select an appropriate set of C-nodes. We provide an adaptive algorithm based on a bit error rate criteria. The system using the proposed algorithm is evaluated by computer simulation in the network with and without interference. From the results, the system using our proposed algorithm can reduce the traffic load and provide good transmission performance, because it selects a set of co-operative nodes adaptively according to SNR of the link.

Implementation of Mobile PPC Realizing Mobility of Mobile Nodes

Masaki Sejimo, Akira Watanabe

We have proposed a new communication system called Mobile PPC (Mobile Peer to Peer Communication), which can keep their connections during their communications even though they change their locations, without using any extra devices. We have implemented Mobile PPC in IP layer, and evaluated the system.

Wed2-5 : Sequences

Correlation Distribution of Quadriphase ZCZ Sequences Obtained from a Perfect Sequence and a Unitary Matrix

Shuichi Jono, Satoshi Uehara

A class of zero-correlation zone (ZCZ) sequences constructed by the recursive procedure from a perfect sequence and a unitary matrix was proposed by Torii, Nakamura, and Suehiro. In the reference, properties of just enough for the class of sequences used in approximately synchronized CDMA (AS-CDMA) systems were considered. In this paper, we give more detailed distributions of correlation values for their ZCZ sequence sets, and expect that the results make an effect on any applications employing AS-CDMA systems.

Higher Dimensional Complete-Complementary Sequences: A General Approach

R. S. Raja Durai, Naoki Suehiro

In many applications in image, communications, signal processing, the notion of two-dimensional sequences are widely investigated. This paper focuses on sets of n-dimensional sequences that constitute a complete-complementary codes of sequences. A novel method to construct a class of n-dimensional complete-complementary codes of order N_o and size $M_{n-1} \times M_{n-2} \times \cdots \times M_o$ with $M_{n-1} \leq M_{n-2} \leq \cdots \leq M_o$ is presented. Since an n-dimensional complete-complementary sequences requires only the shorter-length complementary sequences, it has a possitive impact on modulation scheme requirements under some circumstances. The advantage of an n-dimensional complete-complementary sets of sequences is that it increases the maximum user count and processing gain for a given sequence size. What remains is to define a suitable n-dimensional channel over which the n-dimensional complete-complementary sets of sequences can be implemented.

On the Relationship of Sidel'nikov Sequences

Tae-Hyung Lim, Young-Sik Kim, Jung-Soo Chung, Jong-Seon No

In this paper, the relationship among M-ary Sidel'nikov sequences generated by different primitive elements and decimation are studied. Their autocorrelation function and autocorrelation distribution are derived. It is proved that Sidel'nikov sequences for a given period are equivalent under the decimation, cyclic shift, and scalar multiplication of the sequence.

Author Index

Y

Z