様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　２２　日現在

機関番号：　２０１０３
研究種目：　基盤研究(B)（一般）
研究期間：　2015～2017
課題番号：　１５Ｈ０２６９２

研究課題名（和文）モバイルアドホックネットワークの秘密容量に関する研究

研究課題名（英文）Secrecy Capacity Study for Mobile Ad Hoc Networks

研究代表者

ＪＩＡＮＧ　Ｘｉａｏｈｏｎｇ（Jiang, Xiaohong）

公立はこだて未来大学・システム情報科学部・教授

研究者番号：００３４５６５４

交付決定額（研究期間全体）：（直接経費）　　7,900,000円

研究成果の概要（和文）：本研究プロジェクトでは，MANETの秘密容量（SC）に関して，正確なSCの分析，SC/遅延/機能停止のトレードオフ，SCの増大/最適化の3つの基本的な問題の調査を行った．セル分割されたMANETs，時間スロット化されたMANETs，そして，大規模無線ネットワークのSCを調査した．秘密機能停止確率と伝送機能停止確率のモデリング，遅延のモデリング，そして，SC，遅延，機能停止性能間の固有のトレードオフについての研究を行った．SCの最大化を目的に，リンク選択ポリシーの最適なパラメータ設定，最適なモード選択とスペクトラム分割，そして，メッセージ伝送電力とノイズ伝送電力の最適制御に関する調査を行った．

研究成果の概要（英文）：This project investigated the three fundamental issues of MANET secrecy capacity (SC) study, namely the exact SC analysis, SC/delay/outage tradeoff and SC enhancement/optimization. About the exact SC study, we explored SC of cell-partitioned MANETs with group-based transmission scheduling, time-slotted MANETs with secure Aloha MAC protocol, and large-scale wireless networks with the consideration of social relationships among nodes. About SC/delay/outage tradeoff, we studied the modeling of secrecy outage probability and transmission outage probability, modeling of delay, and the inherent trade-offs among the security, delay and outage performances. About capacity enhancement/optimization, we explored the optimal parameter settings of the link selection policies for the maximization of SC, the optimal mode selection and spectrum partition for SC maximization, and the optimal control of message transmission power and noise transmission power for SC maximization.

研究分野：　総合領域

キーワード：　MANET　秘密容量　物理層のセキュリティ

１．研究開始当初の背景

The flexible MANETs are highly appealing for many important applications, like the disaster recovery networks, emergency networks and sensor networks. The well-known Wyner's secrecy capacity (SC) theory, which is built on the classic Shannon security notion and has been vital for characterizing the link SC, is not well suited to characterize the SC of decentralized MANETs. Thus, despite much research activity on MANETs, the MANET SC theory - a theory defining the maximum secrecy rates achievable between all node pairs, has remained an open problem. The promising PHY security technologies (like artificial noise, cooperative jamming and beam-forming), which exploit the inherent randomness of channels and noise for secret communication, have recently attracted considerable attention since they characterize the fundamental ability of PHY to provide everlasting and a strong form of security guarantee against eavesdroppers. This is why there is a renewed interest in developing a powerful PHY security-based SC theory for MANETs, as evident from several ongoing national-scale projects in the USA and Europe. It is expected that such a theory not only helps us to understand the basic network SC limit but also serves as an instruction guideline for the design and optimization of future secure MANETs. Therefore, we envision that the study of a general MANET SC theory will solidly contribute to the development of modern Network Information Theory and the continuing success of future secure communication networks.

２．研究の目的

The goal of this project is to research on the three fundamental issues of MANET SC study in the context of PHY security, namely the exact SC analysis, SC/delay/outage tradeoff and SC enhancement/optimization. We first study the exact SC of various MANET scenarios with different secure transmission protocols and different eavesdropper models. The main PHY security technologies to be considered include artificial noise, cooperative jamming and link-selection. Second, we explore the exact SC/delay/outage tradeoff under various network scenarios with different types of relays, different eavesdropper models, different channel state information (CSI). Some new secure routing/transmission schemes are developed for a flexible SC/delay/outage tradeoff. Finally, we explore the design of the link-selection, spectrum partition, transmission power control for SC enhancement/optimization.

３．研究の方法

(1) SC Study: For discrete cell-partitioned MANETs with group-based transmission scheduling, we first developed some secure transmission schemes based on the PHY security technology, then we applied the Lyapunov Drift Theory to establish a general theoretical framework for SC evaluation of such MANET under a given secure transmission scheme. For a time-slotted MANET with continuous square area and torus boundaries, we first proposed a secure Aloha protocol based on the PHY security technology technique, and then applied the Lyapunov Drift Theory and stochastic geometry theory to establish a complete theoretical framework for its SC capacity study and for exploring the corresponding SC maximization problem. Based these studies, we further explore the SC study of practical large-scale wireless networks with the consideration of social relationships among nodes, where legitimate nodes may be homogeneously distributed based on a Poisson point process, or in-homogeneously distributed as multi-clustering topology, and eavesdroppers can be non-colluding or colluding.

(2) SC/Delay/Outage Tradeoff: With the help of Statistical Theory and the techniques of Laplace transform, keyhole contour integral and Cauchy Integral Theorem, we first developed different theoretical frameworks for the modeling of secrecy outage probability (SOP) and transmission outage probability (TOP) under different network scenarios, like the two-hop relay networks, multi-hop wireless ad hoc networks and large-scale wireless networks. We then combined the theories of fixed-point, quasi-birth-and-death process, embedded Markov chain and the absorbing Markov chain theory to develop a general theoretical framework for the delay modeling of practical buffer-limited MANETs under different MAC protocols. Based on the results of SC analysis, SOP modeling and delay modeling, we explore the inherent trade-offs among them under different network scenarios. We also apply different PHY security techniques to develop new secure routing/transmission schemes to enable a flexible trade-off to be initiated among security, delay and outage performances.

(3) SC Optimization/Enhancement: For a buffer-aided two-hop cooperative wireless network, we first proposed novel link selection policies to enhance the security of the network, and then apply the Constrained Nonlinear Optimization (CNO) to develop theoretical frameworks for the optimization of SC and SOP of the network under the new link selection policies. For cellular networks with in-band device-to-device (D2D) communication, we apply the Nonlinear Optimization to develop a

general theoretical framework to identify the optimal mode selection of D2D pairs and optimal spectrum partition between cellular users and overlay D2D communications, such that system SC can be maximized. For an Aloha MANET, we first proposed a new secure Aloha protocol based on the PHY security technique of artificial noise. We then apply the CNO to develop a theoretical framework to identify optimal control of the message transmission power and noise transmission power such that the SC of such a secure Aloha MANET can be maximized.

４．研究成果

(1) Exact SC Study

① For cell-partitioned MANETs with group-based transmission scheduling scheme, we first proposed two secure transmission schemes based on the PHY security technology, i.e., secrecy guard zone based and cooperative jamming-based schemes. We then developed the theoretical frameworks to derive the exact analytical expressions for the SC of the concerned network under both secure transmission schemes based on the analysis of basic secure transmission probabilities therein.

② For a time-slotted MANET with continuous square area and torus boundaries, we establish a complete theoretical framework for its capacity study when Aloha MAC protocol is adopted. We then proposed a secure and traffic-independent Aloha protocol based on the PHY security technology technique of artificial noise, and further derived the exact analytical expression for the SC performance of the concerned network under the secure Aloha protocol and also explored the corresponding SC maximization problem.

③ We studied the SC of large-scale wireless networks with the consideration of social relationships among nodes, where legitimate nodes may be homogeneously distributed based on a Poisson point process, or in-homogeneously distributed as multi-clustering topology. In particular, we considered two scenarios, the non-colluding case where each eavesdropper decodes its receiving message independently, or the colluding case, where eavesdroppers can cooperate to decode the message.

(2) Secure Routing/Transmission Schemes

① For a buffer-aided two-hop relay wireless network, we proposed cooperative jamming schemes for both perfect and partial CSI cases of eavesdropper. Based on the channels qualities, two relays are selected in each hop, one is selected as a message relay and another as a jammer to transmit jamming signals to degrade the eavesdropper channel. Optimal relay selection problem is also explored for the maximization of SC. We further proposed new buffer-aided relay selection scheme to resist the eavesdropper's combining decoding when Decode-and-Forward (DF) relays are adopted. Finally, in a finite Poisson wireless network with social friendships among nodes, a social friendship-based cooperative jamming scheme is proposed against eavesdroppers. The jamming scheme consists of a Local Friendship Circle (LFC) and a Long-range Friendship Annulus (LFA), where all legitimate nodes in the LFC serve as jammers, but the legitimate nodes in the LFA are selected as jammers through some location-based policies.

② For a multi-hop wireless ad hoc network (WANET), we proposed a secure routing algorithm which can achieve the optimal security-QoS tradeoffs for any pair of source and destination nodes in a distributed manner. We further considered a WANET with malicious eavesdroppers and cooperative jammers, and proposed an optimal secure routing algorithm which selects the secure path between a pair of source and destination nodes to achieve the optimal QoS performance. Finally, we considered a WANET with the typical amplify-and-forward (AF) and decode-and-forward (DF) transmission schemes, and proposed a flexible routing selection algorithm which enables us to select the suitable route for message delivery according to different security and QoS requirements under the AF or DF scheme.

③ For a cell-partitioned MANET with group-based scheduling scheme, we proposed two secure transmission schemes based on the PHY security technology, i.e., secrecy guard zone based and cooperative jamming based. The secrecy guard zone-based scheme allows transmissions to be conducted only if no eavesdroppers exist in the secrecy guard zone around transmitters. The cooperative jamming-based scheme utilizes non-transmitting nodes to generate artificial noise to suppress eavesdroppers in the same cell, such that transmissions can be conducted only if all eavesdroppers in the transmission range are suppressed. For a time-slotted MANET with continuous square area and torus boundaries, we proposed the secure Aloha protocol based on the technique of artificial noise. For the secure Aloha protocol, legitimate transmitter produces artificial noise to help masking the confidential message transmissions. Artificial noise is utilized to impair the eavesdropper's channel, but it does not affect the intended receiver's channel since the noise is generated in the null-subspace of the

legitimate receiver's channel.

(3) SC/Delay/Outage Tradeoff

① We developed solid theoretical frameworks for the modeling of secrecy outage probability (SOP) and transmission outage probability (TOP) in two-hop wireless networks under different scenarios, like the ones with/without buffer-aided relays, the ones with/without full CSI information, the ones with randomize-and-forward (RF) relays or Decode-and-Forward (DF) relays, and ones with non-colluding or colluding eavesdroppers. We also developed theoretical model for the SOP of secure multicasting. For a finite Poisson wireless network with social friendships among nodes, both the upper and lower bounds on the SOP are developed under a social friendship-based cooperative jamming scheme. Finally, we derived in closed-form the end-to-end SOP and TOP in multi-hop wireless ad hoc networks under various scenarios, like the ones containing malicious eavesdroppers and cooperative jammers, and the ones adopting the typical amplify-and-forward AF and DF transmission schemes.

② For two-hop buffer-aided relay wireless networks, we applied the absorbing Markov chain theory and the Queuing theory to derive the analytical expressions for the end-to-end delay (E2E) under both perfect and partial CSI cases and both scenarios of RF relays or DF relays. We developed a quasi-birth-and-death approach for the E2E modeling in MANETs, and further combined the theories of fixed-point, quasi-birth-and-death process, embedded Markov chain and the absorbing Markov chain theory to develop a general theoretical framework for the E2E delay modeling for buffer-limited MANETs under different MAC protocols. We also explored the packet delivery delay modeling issue for the three-dimensional MANETs.

③ For a two-hop buffer-aided relay wireless networks, we explored the inherent trade-off between the E2E security and delay performances there under both perfect and partial CSI cases and both scenarios of RF relays or DF relays. The results indicate that the E2E security performance increases as the constraint on the expected E2E delay becomes less strict, on the other hand, the E2E delay tends to decrease when a less strict constraint on security performance is imposed. For a buffer-aided two-hop cooperative wireless network, we further explored trade-offs between SC and secrecy outage probability (SOP). We also explored the trade-offs between security performance (defined by SOP) and QoS performance (defined by connection outage probability-COP) in wireless ad hoc networks to minimize COP (resp. SOP) conditioned on that SOP (resp. COP) is guaranteed under two typical transmission schemes of AF and DF.

(4) SC Optimization/Enhancement

① For a buffer-aided two-hop cooperative wireless network, we proposed novel link selection policies to enhance the security of the network, which conducts source-to-relay link selection, relay-to-destination link selection, or no link transmission based on the channels qualities. We then established theoretical frameworks for exploring the issues of optimal parameter settings of the proposed link selection policies for the maximization of secrecy outage capacity, maximization of end-to-end secrecy throughput, and minimization of secrecy outage probability.

② For cellular networks with in-band device-to-device (D2D) communication, we investigated from the PHY security perspective the fundamental issues of mode selection and spectrum partition in such network. In particular, we first developed a general theoretical framework to model both the secrecy outage/secrecy capacity performance of cellular users and outage/capacity performance of D2D pairs, and then explored the performance optimization issues to identify the optimal mode selection and spectrum partition for secrecy capacity maximization and secrecy outage probability minimization.

③ We first proposed a secure Aloha protocol based on the technique of artificial noise for MANETs, where the legitimate transmitter produces artificial noise to help masking the confidential message transmissions, and artificial noise is utilized to degrade the eavesdropper's channel. We derived exact analytical expression for the secrecy throughput capacity (STC) of the concerned network under the secure Aloha protocol, and further explored the optimal control of the message transmission power and noise transmission power such that the STC of such a secure Aloha MANET can be maximized.

５．主な発表論文等

〔雑誌論文〕（計 23 件, 査読有）

[1] Yuanyu Zhang, Yulong Shen, Hua Wang, Yanchun Zhang and Xiaohong Jiang, On Secure Wireless Communications for Service Oriented Computing, IEEE Transactions on Services Computing, vol.11, no.2, pp. 318-328, March/April 2018.
DOI: 10.1109/TSC.2015.2478453

[2] Yuanyu Zhang, Yulong Shen, Hua Wang and Xiaohong Jiang, Friendship-based Cooperative Jamming for Secure Communication in Poisson Networks, Wireless Networks, vol.10, pp.1-19,

May 2018. DOI: 10.1007/s11276-018-1732-1
[3] Kechen Zheng, Ying Cui, Xiaoying Liu, Xinbing Wang and Xiaohong Jiang, Asymptotic Analysis of Inhomogeneous Information-Centric Wireless Networks with Infrastructure Support, IEEE Transactions on Vehicular Technology, Feb.2018. DOI: 10.1109/TVT.2018.2810312
[4] Xiaochen Li, Shuangrui Zhao, Yuanyu Zhang, Yulong Shen and Xiaohong Jiang, Exact Secrecy Throughput Capacity Study in Mobile Ad Hoc Networks, Ad Hoc Networks, vol.72, pp.105–114, April 2018. DOI: 10.1016/j.adhoc.2018.01.012
[5] Bin Yang, Yulong Shen, Xiaohong Jiang and Tarik Taleb, Generalized Cooperative Multicast in Mobile Ad Hoc Networks, IEEE Transactions on Vehicular Technology, vol.67, no. 3, pp.2631 – 2643, March 2018.
DOI: 10.1109/TVT.2017.2771286
[6] Wu Wang, Bin Yang, Osamu Takahashi, Xiaohong Jiang, and Shikai Shen, On the Packet Delivery Delay Study for Three-Dimensional Mobile Ad Hoc Networks, Ad Hoc networks, vol.69, pp.38-48, Feb.2018.
DOI: 10.1016/j.adhoc.2017.10.004
[7] Xuening Liao, Yuanyu Zhang, Zhenqiang Wu, Yulong Shen, Xiaohong Jiang and Hiroshi Inamura, On Security-Delay Trade-off in Two-Hop Wireless Networks with Buffer-Aided Relay Selection, IEEE Transactions on Wireless Communications, vol.17, no.3, pp.1893 – 1906, March 2018. DOI: 10.1109/TWC.2017.2786258
[8] Jia Liu, Yang Xu, Yulong Shen, Xiaohong Jiang, and Tarik Taleb, On Performance Modeling for MANETs under General Limited Buffer Constraint, IEEE Transactions on Vehicular Technology, pp.9483 – 9497, vol.66, no.10, Oct. 2017.
DOI: 10.1109/TVT.2017.2710099
[9] Yang Xu, Jia Liu, Yulong Shen, Xiaohong Jiang, and Norio Shiratorid, Physical Layer Security-Aware Routing and Performance Tradeoffs in Ad Hoc Networks, Computer Networks, vol.123, pp.77–87, Aug. 2017.
DOI: 10.1016/j.comnet.2017.05.012
[10] Yin Chen, Jinxiao Zhu, Yulong Shen, Xiaohong Jiang, and Hideyuki Tokuda, On the Rate of Successful Transmissions in Finite Slotted Aloha MANETs, Ad Hoc networks, vol.62, pp.76–87, July 2017.
DOI: 10.1016/j.adhoc.2017.04.005
[11] Kechen Zheng, Jinbei Zhang, Xiaoying Liu, Luoyi Fu, Xinbing Wang, Xiaohong Jiang, and Wenjun Zhang, Secrecy Capacity Scaling of Large-Scale Networks with Social Relationships, IEEE Transactions on Vehicular Technology, vol.66, no,.3, pp. 2688 - 2702, March 2017.
DOI: 10.1109/TVT.2016.2582778
[12] Yang Xu, Jia Liu, Yulong Shen, Xiangning Li, and Xiaohong Jiang, On throughput capacity of large-scale ad hoc networks with realistic buffer constraint, Wireless Networks, vol.23, no.1, pp 193–204, Jan.2017.
DOI:10.1007/s11276-015-1146-2
[13] Yujian Fang, Yuezhi Zhou, Xiaohong Jiang, and Yaoxue Zhang, Practical Performance of MANETs under Limited Buffer and Packet Lifetime, IEEE Systems Journal, vol.11, no.2, pp.995-1005, June 2017.
DOI: 10.1109/JSYST.2015.2473155
[14] Yin Chen, Yulong Shen, Jinxiao Zhu, Xiaohong Jiang, and Hideyuki Tokuda, On the Throughput Capacity Study for Aloha Mobile Ad Hoc Networks, IEEE Transactions on Communications, vol.64, no.4, pp.1646 – 1659, April 2016.
DOI: 10.1109/TCOMM.2016.2527658
[15] Yuanyu Zhang, Yulong Shen, Hua Wang, and Xiaohong Jiang, On Secure Wireless Communications for IoT under Eavesdropper Collusion, IEEE Transactions on Automation Science and Engineering, vol.13, no.3, 1281-1293, July 2016.
DOI: 10.1109/TASE.2015.2497663
[16] Jia Liu, Min Sheng, Jiandong Li and Xiaohong Jiang, On Throughput Capacity for a Class of Buffer-Limited MANETs, Ad Hoc Networks, vol.37, pp.354-367, Jan.2016
DOI:10.1016/j.adhoc.2015.08.029
[17] Jia Liu, Ming Sheng, Yang Xu, Jiandong Li, and Xiaohong Jiang, End-to-end Delay Modeling in Buffer-Limited MANETs: A General Theoretical Framework, IEEE Transactions on Wireless Communications, vol.15, no.1, pp.498-511, Jan.2016.
DOI: 10.1109/TWC.2015.2475258
[18] Juntao Gao, Yulong Shen, Xiaohong Jiang, Osamu Takahashi and Norio Shiratori, End-to-End Delay Modeling for Mobile Ad Hoc Networks: A Quasi-Birth-and-Death Approach, Ad Hoc & Sensor Wireless Networks, vol.29, no.1-4, pp.265-285, 2015.
[19] Yuanyu Zhang, Yulong Shen, Jinxiao Zhu and Xiaohong Jiang, Eavesdropper-Tolerance Capability in Two-Hop Wireless Networks via Cooperative Jamming, Ad Hoc & Sensor Wireless Networks, vol.29, no.1-4, pp.113-131, 2015.
[20] Bin Yang, Yin Chen, Guilin Chen, and Xiaohong Jiang, Throughput Capacity Study for MANETs with Erasure Coding and Packet Replication, IEICE Transactions on Communications, vol.E98-B, no.8, pp.1537-1552, Aug.2015. DOI: 10.1587/transcom.E98.B.1537
[21] Bin Yang, Ying Cai, Yin Chen and Xiaohong

Jiang, On the Exact Multicast Delay in Mobile Ad Hoc Networks with f-cast Relay, Ad Hoc Networks, vol.33, pp.71–86, Oct.2015.
DOI: 10.1016/j.adhoc.2015.04.005
[22] Yin Chen, Yulong Shen, Jinxiao Zhu, and Xiaohong Jiang, Capacity and Delay-Throughput Tradeoff in ICMNs with Poisson Contact Process, Wireless Networks, vol.21, no.8, pp.2453-2466, Nov.2015. DOI: 10.1007/s11276-015-0926-z
[23] Bin Yang, Yin Chen, Ying Cai and Xiaohong Jiang, Packet Delivery Ratio/Cost in MANETs with Erasure Coding and Packet Replication, IEEE Transactions on Vehicular Technology, vol.64, no.5, pp.2062-2070, May 2015.
DOI: 10.1109/TVT.2014.2362355

〔学会発表〕（計 13 件, 査読有）

[1] Huihui Wu, Xuening Liao, Yongchao Dang, Yulong Shen and Xiaohong Jiang, Limits of Covert Communication on Two-Hop AWGN Channels, 2017 International Conference on Networking and Network Applications (NaNA 2017), July 16-19, 2017, Kathmandu City, Nepal
[2] Yeqiu Xiao, Jia Liu, Jiao Quan, Yulong Shen and Xiaohong Jiang, On Secrecy Performance of Multibeam Satellite System with Multiple Eavesdropped Users, 13th International Conference on Mobile Ad-hoc and Sensor Networks, Dec.17-20, 2017, Beijing, China.
[3] Kenta Sasaki, Xuening Liao and Xiaohong Jiang, Cooperative Jamming in a Two-Hop Relay Wireless Network with Buffer-Aided Relays, CANDAR 2017- WANC workshop, Nov.19-22, 2017, Aomori, Japan.
[4] Shuangrui Zhao, Jia Liu, Xiaochen Li, Yulong Shen and Xiaohong Jiang, Secure Beamforming for Full-duplex MIMO Two-way Communication via Untrusted Relaying, IEEE GLOBECOM 2017 Workshops: The First IEEE Workshop on PHY and Cross-Layer Security Solutions for 5G Networks, 4-8 Dec.2017, Singapore
[5] Yujian Fang, Yuezhi Zhou, Xiaohong Jiang, Di Zhang and Yaoxue Zhang, Game Theoretic D2D Content Sharing: Joint Participants Selection, Routing and Pricing, IEEE ICCCN 2017, 31 July-3 Aug. 2017, Vancouver, Canada.
[6] Yang Xu, Jia Liu, Osamu Takahashi, Xiaohong Jiang and Norio Shiratori, SOQR: Secure Optimal QoS Routing in Wireless Ad Hoc Networks, IEEE WCNC 2017, 19-22 March 2017, San Francisco, USA.
[7] Yang Xu, Jia Liu, Yulong Shen, Xiaohong Jiang, and Tarik Taleb, Security/QoS-Aware Route Selection in Multi-hop Wireless Ad Hoc Networks, IEEE ICC 2016, 23-27 May 2016, Kuala Lumpur, Malaysia.
[8] Wu Wang, Bin Yang, Osamu Takahashi, Xiaohong Jiang, and Shikai Shen, Delivery Probability of 3D MANETs with Packet Replication, NaNA 2016, July 23-25, 2016, Hakodate City, Japan.
[9] Ji He, Yuanyu Zhang, Yulong Shen, and Xiaohong Jiang, Link Selection for Secure Two-Hop Transmissions in Buffer-Aided Relay Wireless Networks, NaNA 2016, July 23-25, 2016, Hakodate City, Japan.
[10] Xiaochen Li, Shuangrui Zhao, Yuanyu Zhang, Yulong Shen, and Xiaohong Jiang, Exact Secrecy Throughput of MANETs with Guard Zone, NaNA 2016, July 23-25, 2016, Hakodate City, Japan.
[11] Xuening Liao, Zhenqiang Wu, Yuanyu Zhang, and Xiaohong Jiang, The Delay-Security Trade-Off in Two-Hop Buffer-Aided Relay Wireless Network, NaNA 2016, July 23-25, 2016, Hakodate City, Japan.
[12] Wu Wang, Bin Yang, Xiaohong Jiang and Osamu Takahashi, Delivery Delay in 3D MANETs with Packet Redundancy, CANDAR 2015, Dec.8-11, 2015, Sapporo, Japan.
[13] Chungang Yang, Jiandong Li, Xiaohong Jiang and Alagan Anpalagan, Interference-Aware Spectral-and-Energy Efficiency Tradeoff in Heterogeneous Networks, 2015 IEEE WCNC, 9-12 March, 2015, New Orleans, USA.

６．研究組織

(1)**研究代表者**

姜　暁鴻　（JIANG　Xiaohong）
公立はこだて未来大学・システム情報科学部・教授
研究者番号：00345654

(2)**研究分担者**

福士　将　（FUKUSHI Masaru）
山口大学・理工学研究科・准教授
研究者番号：50345659

(3)**研究分担者**

高橋　修　（TAKAHASHI Osamu）
公立はこだて未来大学・システム情報科学部・教授
研究者番号：60381282