REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
08-10-2021	Final Report	25-Sep-2017 - 24-Jul-2021

4. TITLE AND SUBTITLE
Final Report: Secure Wireless Network with Full-Duplex Radio

5a. CONTRACT NUMBER
W911NF-17-1-0581

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of California - Riverside
200 University Office Building

Riverside, CA 92521 -0001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
69739-NS-H.20

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Yingbo Hua
UU	UU	UU	UU		19b. TELEPHONE NUMBER 951-827-2853

RPPR Final Report
as of 18-Oct-2021

Agency Code: 21XD

Proposal Number: 69739NSH **Agreement Number: W911NF-17-1-0581**
INVESTIGATOR(S):

Name: Yingbo Hua
Email: yhua@ucr.edu
Phone Number: 9518272853
Principal: Y

Organization: **University of California - Riverside**
Address: 200 University Office Building, Riverside, CA 925210001
Country: USA

DUNS Number: 627797426 EIN: 956006142
Report Date: 24-Oct-2021 Date Received: 08-Oct-2021
Final Report for Period Beginning 25-Sep-2017 and Ending 24-Jul-2021
Title: Secure Wireless Network with Full-Duplex Radio
Begin Performance Period: 25-Sep-2017 **End Performance Period:** 24-Jul-2021
Report Term: 0-Other

Submitted By: Yingbo Hua Email: yhua@ucr.edu
Phone: (951) 827-2853

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 3 **STEM Participants:** 5

Major Goals: This project aims to develop much improved understanding of the potential of full-duplex radio for secure wireless network, and to develop real-time computational methods for power allocation and beamforming to maximize the security of wireless network equipped with full-duplex radio subject to little or no penalty on user experience. We consider the scenario where full-duplex radio is used to provide the first line of defense at the physical layer of wireless network against eavesdropping from enemy. The full-duplex mode in any given full-duplex radio is treated as dynamically switchable (enabled or disabled) according to user's need. The residual self-interference in full-duplex radio is fully taken into account in maximization of secrecy capacity subject to rate, power and/or other constraints. We consider cases where social network and wireless network are treated holistically so that human needs are best served. One particular example is where military radio and civilian radio coexist to improve the efficiency in utilizing limited radio spectrum but without compromising security. The network and channel information readily available for communications among radios for common civilian purposes is utilized to provide additional security for communicating sensitive information.
We will develop new insights into fundamental tradeoffs among network throughput, security, network and channel information, and computational complexity. Various network settings, from a three-node building block to networks of many nodes, will be explored. Broadband multicarrier systems as well as multiple-antenna radio will be considered. Fast computational algorithms for non-convex optimization problems arising from secure wireless network with full-duplex radio will be developed and thoroughly evaluated so that future FPGA implementation on programmable radio boards for real-time testing becomes feasible.

Accomplishments: to be uploaded later

Training Opportunities: Nothing to Report

Results Dissemination: Nothing to Report

Honors and Awards: Associate Editor, IEEE Transactions on Signal and Information Processing over Networks, April 2017 – April 2021.

Senior Area Editor, IEEE Transactions on Signal Processing, Feb 2016 – Feb 2020.

Chair, Steering Committee for IEEE Wireless Communication, Jan 2020 -.

Member, Steering Committee for IEEE Wireless Communication Letters, Jan 2016 – Dec 2019.

Lead Chair, IEEE GlobalSIP Symposium on Signal Processing for Wireless Network Security, Anaheim, CA, USA, Nov 2018.

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: Graduate Student (research assistant)
Participant: Reza Sohrabi
Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Qiping Zhu
Person Months Worked: 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Shuo Wu
Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Ishman Zabir
Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Ahmed Maksud
Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
National Academy Member: N

RPPR Final Report
as of 18-Oct-2021

ARTICLES:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Signal Processing
Publication Identifier Type: DOI Publication Identifier: 10.1109/TSP.2018.2879621
Volume: 67 Issue: 1 First Page #: 120
Date Submitted: 8/13/19 12:00AM Date Published: 1/1/19 4:00PM
Publication Location: United States
Article Title: Advanced Properties of Full-Duplex Radio for Securing Wireless Network
Authors: Yingbo Hua
Keywords: Wireless network security, full-duplex radio, antieavesdropping channel estimation, mobile ad hoc network, drone network, multi-agent network.
Abstract: This paper first studies the secrecy capacity of two single-antenna full-duplex users against a multi-antenna eavesdropper (Eve) who has the perfect knowledge of its channel state information (CSI) from users to Eve. It is shown that if Eve uses a basic matched-filtering, the probability of secrecy outage can be made small by a large jamming power from both users and a small gain of residual self-interference (RSI) power. But if Eve uses the optimal matched-filtering, that probability grows rapidly as either the jamming power from the users increases or the number of antennas on Eve increases, regardless of the RSI gain. To prevent any Eve from obtaining its CSI, this paper then proposes a novel anti-eavesdropping channel estimation (ANECE) method, which allows users to obtain their own CSI while keeping all Eves in handicap. It is shown that the capacity of Eve with any number of antennas but without its CSI can be virtually eliminated over a time window for each CSI realization.
Distribution Statement: 3-Distribution authorized to U.S. Government Agencies and their contractors
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: N **Publication Status:** 1-Published
Journal: arXiv
Publication Identifier Type: Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 8/13/18 12:00AM Date Published: 11/27/17 8:00AM
Publication Location:
Article Title: Fundamental Properties of Full-Duplex Radio for Secure Wireless Communications
Authors: Yingbo Hua, Qiping Zhu, Reza Sohrabi
Keywords: Wireless Security, Full-Duplex Radio, Secrecy Capacity Field
Abstract: This paper considers the fields of secrecy capacity of a wireless channel between two single-antenna radios (Alice and Bob) against an unknown number of single-antenna eavesdroppers (Eves) from unknown locations. Important properties discovered in this paper show: how the secrecy capacity of this channel is distributed in terms of the location of Eve, how the optimal jamming power applied by the full-duplex radio varies with various parameters, and how bad or good the worst cases are. In particular, these properties show how the quality of self-interference cancelation/suppression on the full-duplex radios affects various aspects of the fields of secrecy capacity.
Distribution Statement: 3-Distribution authorized to U.S. Government Agencies and their contractors
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 18-Oct-2021

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 4-Under Review
Journal: IEEE Transactions on Signal Processing
Publication Identifier Type: Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 8/13/19 12:00AM Date Published:
Publication Location:
Article Title: Perfect Unconditional Secrecy for Network Security
Authors: Yingbo Hua
Keywords: Network security, physical layer security, unconditional secrecy, anti-eavesdropping channel estimation, reciprocal channel modulation, random modulation
Abstract: This paper addresses secrecy of information transmission against eavesdroppers (Eves) unconditional upon their numbers of antennas. This unconditional secrecy (UNS) is ideal for network security against Eves. But all previous physical layer security schemes including secret information transmission (SIT) schemes and secret key generation (SKG) schemes have their UNS rates (if any) decreasing to zero as channel coherence time (CCT) and/or channel coherence bandwidth (CCB) increase. This paper presents a new class of SIT schemes called reciprocal channel modulation (RCM) schemes for two or more devices with or without multiple antennas. The RCM schemes embedded with random modulation achieve constant UNS rates in both time and frequency, i. e., constant UNS bits per second per Hertz even as CCT and/or CCB increase. Furthermore, the RCM schemes can also achieve perfect UNS rates equal to any data rates chosen for the packets transmitted between devices.
Distribution Statement: 3-Distribution authorized to U.S. Government Agencies and their contractors
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Signal Processing
Publication Identifier Type: DOI Publication Identifier: 10.1109/TSP.2019.2949501
Volume: 67 Issue: 23 First Page #: 5968
Date Submitted: 8/11/20 12:00AM Date Published: 10/25/19 7:00AM
Publication Location: New York
Article Title: Secrecy Analyses of a Full-Duplex MIMOME Network
Authors: Reza Sohrabi, Qiping Zhu, Yingbo Hua
Keywords: Physical layer security, secrecy rate, full-duplex radio, MIMOME, jamming, artificial noise, anti-eavesdropping channel estimation (ANECE).
Abstract: This paper presents secrecy analyses of a full-duplex MIMOME network which consists of two full-duplex multi-antenna users (Alice and Bob) and an arbitrarily located multi-antenna eavesdropper (Eve). The paper assumes that Eve's channel state information (CSI) is completely unknown to Alice and Bob except for a small radius of secured zone. The first part of this paper aims to optimize the powers of jamming noises from both users. To handle Eve's CSI being unknown to users, the focus is placed on Eve at the most harmful location, and the large matrix theory is applied to yield a hardened secrecy rate to work on. The performance gain of the power optimization in terms of maximum tolerable number of antennas on Eve is shown to be significant. The second part of this paper shows two analyses of anti-eavesdropping channel estimation (ANECE) that can better handle Eve with any number of antennas. One analysis assumes that Eve has a prior statistical knowledge of its CSI, which yields low
Distribution Statement: 2-Distribution Limited to U.S. Government agencies only; report contains proprietary info
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 18-Oct-2021

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Signal Processing
Publication Identifier Type: DOI Publication Identifier: 10.1109/TSP.2020.2986307
Volume: 68 Issue: 1 First Page #: 2629
Date Submitted: 8/11/20 12:00AM Date Published: 4/17/20 2:00PM
Publication Location: New York
Article Title: Optimal Pilots for Anti-Eavesdropping Channel Estimation
Authors: Qiping Zhu, Shuo Wu, Yingbo Hua
Keywords: Physical layer security, channel estimation, pilot design.
Abstract: Anti-eavesdropping channel estimation (ANECE) is a method that uses specially designed pilot signals to allow two or more full-duplex radio devices each with one or more antennas to estimate their channel state information (CSI) consistently and at the same time prevent eavesdropper (Eve) with any number of antennas from obtaining its CSI consistently. This paper presents optimal designs of the pilots for ANECE based on two criteria. The first is the mean squared error (MSE) of channel estimation for the users, and the second is the mutual information (MI) between the pilot-driven signals observed by the users. Closed-form optimal pilots are shown under the sum-MSE and sum-MI criteria subject to a symmetric and isotropic condition. Algorithms for computing the optimal pilots are shown for general cases. Fairness issues for three or more users are discussed. The performances of different designs are compared.
Distribution Statement: 2-Distribution Limited to U.S. Government agencies only; report contains proprietary info
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Information Forensics and Security
Publication Identifier Type: DOI Publication Identifier: 10.1109/TIFS.2020.3047763
Volume: 16 Issue: 1 First Page #: 2060
Date Submitted: 10/8/21 12:00AM Date Published: 12/28/20 8:00AM
Publication Location: United States
Article Title: Secrecy of Multi-Antenna Transmission with Full-Duplex User in the Presence of Randomly Located Eavesdroppers
Authors: Ishmam Zabir, Ahmed Maksud, Gaojie Chen, Brian M. Sadler, Yingbo Hua
Keywords: Physical Layer Security, Beamforming, Artificial Noise, Stochastic Geometry, Full Duplex, Secrecy Connectivity, Power Allocation.
Abstract: This paper considers the secrecy performance of several schemes for multi-antenna transmission to single-antenna users with full-duplex (FD) capability against randomly distributed single-antenna eavesdroppers (EDs). These schemes and related scenarios include transmit antenna selection (TAS), transmit antenna beamforming (TAB), artificial noise (AN) from the transmitter, user selection based their distances to the transmitter, and colluding and non-colluding EDs. The locations of randomly distributed EDs and users are assumed to be distributed as Poisson Point Process (PPP). We derive closed form expressions for the secrecy outage probabilities (SOP) of all these schemes and scenarios. The derived expressions are useful to reveal the impacts of various environmental parameters and user's choices on the SOP, and hence useful for network design purposes. Examples of such numerical results are discussed.
Distribution Statement: 3-Distribution authorized to U.S. Government Agencies and their contractors
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 18-Oct-2021

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 4-Under Review
Journal: IEEE Transactions on Signal Processing
Publication Identifier Type: Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 10/8/21 12:00AM Date Published:
Publication Location:
Article Title: Total Secrecy from Anti-Eavesdropping Channel Estimation
Authors: Shuo Wu, Yingbo Hua
Keywords: Wireless networks, physical layer security, antieavesdropping channel estimation, secret key generation, secret information transmission, secure degree of freedom, total secure degree of freedom
Abstract: Anti-eavesdropping channel estimation (ANECE) is useful for a network of cooperative full-duplex radio devices/ users. Using ANECE, a secret key can be generated by each pair of users, and additional secret information can be transmitted between a pair of users. This paper analyses the capacity of the secret key based on ANECE, and compares it with that based on the conventional method for channel training. The paper also analyses the secrecy capacity of information transmission using one-way scheme, and compares it with that using two-way schemes. It is shown that the total amount of secrecy generated from ANECE can be substantially larger than that based on the conventional method for channel training assuming that an eavesdropper may have an unlimited number of antennas. The paper also formulates a total secure degree of freedom (TSDoF) of the ANECE based scheme, and compares it with a prior scheme of secret information transmission from a multi-antenna node to another multi-antenna
Distribution Statement: 2-Distribution Limited to U.S. Government agencies only; report contains proprietary info
Acknowledged Federal Support: **Y**

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE GlobalSIP 2018
Date Received: 13-Aug-2019 Conference Date: 27-Nov-2018 Date Published: 26-Nov-2018
Conference Location: Anaheim, CA
Paper Title: A New Look at Secrecy Capacity of MIMOME Using Artificial Noise from Alice and Bob without Knowledge of Eve's CSI
Authors: Reza Sohrabi, Yingbo Hua
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE Globecom
Date Received: 11-Aug-2020 Conference Date: 09-Dec-2019 Date Published: 09-Dec-2019
Conference Location: Waikoloa, HI, USA
Paper Title: Optimal Pilots for Maximal Capacity of Secret Key Generation
Authors: Qiping Zhu, Yingbo Hua
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE Globecom
Date Received: 11-Aug-2020 Conference Date: 09-Dec-2019 Date Published: 09-Dec-2019
Conference Location: Waikoloa, HI, USA
Paper Title: Secure Downlink Transmission to Full-Duplex User Against Randomly Located Eavesdroppers
Authors: Ishmam Zabir, Ahmed Maksud, Brian Sadler, Yingbo Hua
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 18-Oct-2021

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE ICASSP
Date Received: 11-Aug-2020 Conference Date: 08-May-2020 Date Published: 08-May-2020
Conference Location: Barcelona, Spain
Paper Title: Reliable and secure transmission for future networks
Authors: Yingbo Hua
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE SPAWC
Date Received: 11-Aug-2020 Conference Date: 26-May-2020 Date Published: 26-May-2020
Conference Location: Atlanta, GA
Paper Title: Unconditional secrecy and computational complexity against wireless eavesdropping
Authors: Yingbo Hua, Ahmed Maksud
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 2-Awaiting Publicat
Conference Name: MILCOM2021
Date Received: 08-Oct-2021 Conference Date: 29-Nov-2021 Date Published: 29-Nov-2021
Conference Location: San Diego
Paper Title: Anti-Eavesdropping Channel Estimation Using Multi-Antenna Half-Duplex Radios
Authors: Yingbo Hua
Acknowledged Federal Support: **Y**

DISSERTATIONS:

Publication Type: Thesis or Dissertation
Institution: University of California at Riverside
Date Received: 13-Aug-2019 Completion Date: 12/20/18 11:06PM
Title: Jamming Strategies for Secure Wireless Communication
Authors: Reza Sohrabi
Acknowledged Federal Support: **N**

Publication Type: Thesis or Dissertation
Institution: University of California at Riverside
Date Received: 11-Aug-2020 Completion Date: 9/30/19 7:43PM
Title: Physical Layer Security with Full-Duplex Radio in Wireless Networks
Authors: Qiping Zhu
Acknowledged Federal Support: **N**

Publication Type: Thesis or Dissertation
Institution: University of California at Riverside
Date Received: 08-Oct-2021 Completion Date: 6/1/21 8:34PM
Title: Information Security of Wireless Networks with Full-Duplex Radios
Authors: Shuo wu
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 18-Oct-2021

PATENTS:

Intellectual Property Type: Patent Date Received: **13-Aug-2018**
Patent Title: All-Analog and Hybrid Interference Cancellation Using Cables, Attenuators and Power Splitters
Patent Abstract: A radio interference cancellation device that cancels self-interference from a transmitter to a rec
Patent Number: US 9,906,262 B2
Patent Country: USA
Application Date: 27-Jun-2014 Application Status: 3
Date Issued: 27-Feb-2018

Intellectual Property Type: Patent Date Received: **13-Aug-2018**
Patent Title: Methods for Cancellation of Radio Interference in Wireless Communication Systems
Patent Abstract: A full duplex radio includes self-interference cancellation circuitry for reducing self-interference.
Patent Number: US 9,621,221 B2
Patent Country: USA
Application Date: 21-Aug-2014 Application Status: 3
Date Issued: 11-Apr-2017

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Yingbo Hua
Signature Date: 10/8/21 7:15PM

Accomplishments for ARO Grant Number W911NF-17-1-0581

Yingbo Hua

The scientific achievements are mostly documented in the following publications:

[J1] Y. Hua, Q. Zhu, R. Sohrabi, "Fundamental Properties of Full-Duplex Radio for Secure Wireless Communications," http://arxiv.org/abs/1711.10001, 2017.
[J2] Y. Hua, "Advanced Properties of Full-Duplex Radio for Securing Wireless Network," IEEE Transactions on Signal Processing, Vol. 67, No. 1, pp. 120-135, Jan 1, 2019.
[J3] R. Sohrabi, Q. Zhu, Y. Hua, "Secrecy Analyses of a Full-Duplex MIMOME Network," IEEE Transactions on Signal Processing, Vol. 67, No., 23, pp. 5968-5982, Dec. 2019.
[J4] Q. Zhu, S. Wu, Y. Hua, "Optimal Pilots for Anti-Eavesdropping Channel Estimation," IEEE Transactions on Signal Processing, Vol. 68, pp. 2629-2644, 2020.
[J5] I. Zubir, A. Maksud, G. Chen, B. Sadler, Y. Hua, "Secrecy of Multi-Antenna Transmission with Full-Duplex User in the Presence of Randomly Located Eavesdroppers", IEEE Transactions on Information Forensics and Security, Vol. 16, pp. 2060-2075, Dec 2020.
[J6] S. Wu, Y. Hua, "Total Secrecy from Anti-Eavesdropping Channel Estimation," IEEE Transactions on Signal Processing, under review.
[J7] Y. Hua, A. Maksud, "Continuous Encryption Functions for Security Over Networks," IEEE Transactions on Information Forensics and Security, under review.

[C1] R. Sohrabi, Y. Hua, "A new look at secrecy capacity of MIMOME using artificial noise from Alice and Bob without knowledge of Eve's CSI," IEEE GlobalSIP2018, pp. 1291-1295, Nov 2018.
[C2] I. Zubir, A. Maksud, B. Sadler, Y. Hua, "Secure Downlink Transmission to Full-Duplex User Against Randomly Located Eavesdroppers", IEEE GLOBECOM'2019, Waikoloa, Hawaii, Dec 2019.
[C3] Q. Zhu, Y. Hua, "Optimal Pilots for Maximal Capacity of Secret Key Generation," IEEE GLOBECOM'2019, Waikoloa, Hawaii, Dec 2019.
[C4] Y. Hua, "Reliable and secure transmission for future networks," IEEE ICASSP'2020, pp.2560-2564, Barcelona, Spain, May 2020 (Virtual Conference).
[C5] Y. Hua, A. Maksud, "Unconditional Secrecy and Computational Complexity against Wireless Eavesdropping," IEEE SPAWC, Atlanta, GA, May 2020 (Virtual Conference).
[C6] Y. Hua, "Anti-Eavesdropping Channel Estimation Using Multi-Antenna Half-Duplex Radios," IEEE MILCOM 2021, to appear.

These achievements can be grouped as follows:

1. Practical methods for utilizing full-duplex radios for secure wireless communications.
2. Fundamental capacities of full-duplex radios for secure wireless communications.
3. Novel complementary methodologies other than full-duplex radios for secure wireless communications.

In area 1, we have developed a number of effective methods to utilize full-duplex radio for secure wireless communications. These methods include the simple two-phase transmission scheme between a pair of full-duplex radios [J1], the concurrent jamming scheme from both transmitter and receiver [J3], [J5], [C1], [C2], and the anti-eavesdropping channel estimation (ANECE) scheme for any number of cooperative full-duplex radios with any number of antennas [J2], [J4], [J6], [C3]. These methods are all practically feasible although with varying complexities. They are applicable to any radios with full-duplex capabilities. The current technology for self-interference isolation and cancellation already makes full-duplex practical although the range of transmission depends on the quality of self-interference isolation and cancellation.

In area 2, we have developed deep insights into secrecy capacities of full-duplex radios in various settings against adversaries with unlimited computational capacity. These insights include the secrecy capacity of MIMOME network where eavesdropper may have any number of antennas [J3], [J6], [C1], the secrecy capacity of full-duplex transmission against randomly distributed eavesdroppers [J5], [C1], and the total secure degree of freedom of ANECE against any eavesdropper at any location with any number of antennas [J2], [J3], [J6]. These understandings of full-duplex radios are unsurpassed elsewhere. Our group has been a leader in the world community on full-duplex radio for secure wireless communications.

In area 3, we have discovered a number of novel concepts for secure wireless communications, which are complementary to the use of full-duplex radios and other physical layer security schemes. We have developed a concept called continuous encryption [C4], [C5], [J7], which allows a pair of nodes to exploit their noisy estimates of some shared physical feature to direct encrypt their transmitted information before a secret key is successfully generated from the noisy estimates. Continuous encryption has potential advantages such as short latency, which could be complementary to the conventional key based discrete encryption. Another novel method is ANECE based on half-duplex radios [C6]. This method allows secure wireless transmission over a range that is not feasible for full-duplex radios. Both continuous encryption and half-duplex based ANECE are in their infancy, which await further investigations in the near future.

In addition to the scientific achievements, this grant has in part supported 5 Ph.D. students, three of whom have graduated. They are currently employed by the US companies: Stitch Fix, Nokia and Goldman Sachs.