CWIT 2013

Two-Way (True Full-duplex) Wireless

Amir K. Khandani
Electrical and Computer Engineering Department, University of Waterloo, Waterloo, ON, Canada

***Abstract*—Current wireless systems are one-way (similar to walkie-talkies), meaning that disjoint time or frequency segments are used to transmit and to receive. Realization of two-way wireless has challenged the research community for many years. This article[1] establishes the theory and presents practical realization of two-way (true full-duplex) wireless. In contrast to the widely accepted beliefs, it is shown that two-way wireless is not only feasible, but is fairly simple, with virtually no degradation in signal-to-noise-ratio[2]. The innovation is in the antenna design and multiple levels for cancelling self-interference. Methods are developed to support Multiple-Input Multiple-Output (MIMO) two-way transmission, and asynchronous two-way links (useful in networking applications). The developed hardware uses off-the-shelf components, antennas have a simple structure, are omnidirectional (can be directional, if needed), do not suffer from bandwidth limitations, have a small size/spacing, and the increase in overall complexity is minimal. It is shown that two-way wireless can do more than doubling the rate. In particular:**

1) **Facilitates wireless networking. In particular, the ability to handle asynchronous users enables superimposing a half-duplex, low bit rate, low power, easy to detect network for control signaling superimposed (physical overlay, rather than logical) on top of the network of primary full-duplex data links. The superimposed links are separated from the primary full-duplex data links in the code domain, and use time multiplexing plus Carrier Sense Multiple Access (CSMA) among themselves. However, the conventional problems of CSMA are avoided as control links operate in parallel with primary full-duplex data links. The physical layer of control links is designed such that full-duplex data links can detect and cancel the interference caused by the superimposed control links.**
2) **Enhances security through desirable jamming.**
3) **Provides the ground to realize unconditional security (beyond computational or information theoretical security), using a simple method introduced in this article.**
4) **Facilitates multi-node distributed & collaborative signaling, including realization of Network Information Theoretic setups, and cognitive wireless.**
5) **Exploiting feedback, it improves point-to-point throughput, and enables ultra low power transmission.**
6) **Doubles the point-to-point throughput.**

I. Introduction

A communication link with capability to support connections in both transmit and receive directions at the same time and over the entire frequency band is called full-duplex, or two-way. In contrast, a link that can support the connection in only one direction at a time is called one-way or half-duplex. Current wireless systems are one-way and rely on either separate time slots (time division duplex) or separate frequency bands (frequency division duplex) to transmit and to receive. These alternatives have their pros and cons, but both suffer from lack of ability to transmit and receive concurrently over entire frequency band. Even in the context of Orthogonal Frequency Division Multiple Access (OFDMA), where different frequency tones are used to simultaneously service multiple users, there is no method known to use the tones in opposite directions. A similar shortcoming exists in the context of Code Division Multiple Access (CDMA). Although two-way wireless is theoretically possible, its implementation is difficult due to an excessive amount of self-interference, i.e., the interference each transmitter generates to its own receiver(s).

Full-duplex communication is currently used in many applications, e.g., wired telephones, digital subscriber line, wireless with directional antennas, and free-space optics. The impact of full-duplex links in these earlier applications is limited to doubling the rate by providing two symmetrical pipes of data flowing in opposite directions. In contrast, in multi-user wireless systems, due to the broadcast nature of transmission (everyone hears everyone else), full-duplex capability has the potential to do more than merely doubling the rate, e.g., it facilitates networking, collaborative transmission, and security.

To cancel the self-interference in analog domain, an Auxiliary Transmit signal (ATX) is generated from the Primary Transmit signal (PTX) and added to the received signal in the analog domain. Prefiltering, e.g., by pre-weighting coefficients applied to OFDM tones, are calculated for the ATX signal to cancel the self-interference. ATX can be radio frequency (RF) modulated and added to (i.e., coupled with) the received signal in RF domain prior to Low Noise Amplifier (LNA). It can be also added to the received signal in analog base-band prior to Analog-to-Digital converter (A/D), at the cost of using LNA with a larger dynamic range. In addition to cancellation in the analog domain, digital subtraction is deployed at the receive base-band to further reduce the self-interference. In particular, linearity of the Digital-to-Analog converter (D/A) is exploited to subtract the remaining amount of self-interference from the base-band received signal (while maintaining and benefiting from underlying OFDM structure).

Symmetrical transmit and receive antennas are relatively positioned to reduce self-interference. In two dimensions, pair-wise symmetric antennas are proposed which have (theoretically) zero coupling over entire frequency range. The idea of symmetry is generalized to three dimensions. It is shown there exist triple-wise symmetric antennas with zero coupling between any pair. For MIMO transmission, two sets of such antennas (to be used for transmit and receive) can be arranged in three dimensions such that any antenna in one set is decoupled from all the antennas in the other set. Such three dimensional structures can be also implemented in 2.5 dimensions using layers of a Printed Circuit Board (PCB), e.g., by using patch antennas where one arm of antenna is generated through reflection of the other arm in the ground plane. Examples of such a construction are presented where the same patch is used as the transmit antenna, the receive antenna, and the ATX coupler. This construction is also generalized to MIMO. To further simplify the construction for MIMO, a third class of antenna structures are introduced based on placing one set of antennas in the plane of zero electric field of another set, providing low (but non-zero) coupling.

Implementation: RF transmission is based on 802.11 using a 20MHz channel at 2.4 GHz as well as 5Ghz. Transmission power is about 20dbm which is typical for cellular applications. The basic physical layer follows 802.11 in terms of OFDM structure, preamble, synchronization, etc. For hardware implementation,

[1] Supported by Ontario Ministry of Research and Innovation (ORF-RE).
[2] Due to space limitations, see [1] for details on performance measures.

the software defined radio platform by Lyrtech (now Nutaq) is used, and the final outcome has been tested in outdoor and indoor environments, and it essentially works as reliably as a one-way system.

Two-way wireless has been of interest over a relatively long period of time and there have been some other works addressing this problem [1]-[11]. Author's initial interest in this topic started in 2004, followed by a provisional patent in 2005, actual patent filed in 2006, which was issued in 2010 [2]. The starting point for the author's work was to use multiple transmit antennas with transmit beamforming to create a null at the position of a receive antenna. In particular, using two transmit antennas with 180 degree phase shifts to create a null at the position of a receive antenna which is positioned in the middle of the two transmit antennas. The same antenna structure was later rediscovered in [10][11]. Current article presents a more advanced and mature design. The contents of this article have been publicized on-line in April 2012 [1]. There are several critical components contributing to the excellent performance of the method reported here as compared to the results reported by others, and in particular by research teams from Rice [6]-[9] and Stanford [10][11]:

- Analog Active Cancellation exploiting the linearity of D/A with proper training for channel measurement. Overall active cancellation is done in a way that it does no contradict linearity in the cancellation path. As a result active cancellation does not need to be precise and any such lack of precision, which is unavoidable, will be accounted for (subsequently measured) and compensated in the next step in the digital base-band cancellation.
- Antennas are designed to provide (theoretically) zero self interference over the entire frequency range, including support for MIMO. [3].
- Power Amplifier (PA) modeling and compensation.
- Methods to deal with imperfections caused by numerical inaccuracies, such as rounding effect in FFT/IFFT operations, and methods to optimize accuracy in fixed point arithmetic prior to D/A.[4]
- Dealing with mismatches in RF demodulation, in particular clock and phase jitter.[3].

In addition, compared to other research works, this work includes support for MIMO, asynchronous clients and presents several new applications to exploit the potential of two-way in wireless networks (broadcast nature of wireless provides the ground to benefit from two-way connectivity beyond doubling the rate).

II. Two-Way Connectivity

Consider the full-duplex communication network shown in Fig. 1, in which an access point is communicating with multiple clients. The access point employs OFDMA to service multiple users with full-duplex connectivity over each OFDM tone. The access point can also support multiple transmit and multiple receive antennas to further exploit spatial degrees of freedom to increase rate and/or diversity. In addition, the access point supports new incoming clients which can asynchronously join the network (without prior time/frequency synchronization).

ATX signal is added to the receive chain to reduce the self-interference in analog domain prior to A/D (preferably prior to LNA). ATX signal can be constructed by weighting each OFDM tone of TX signal by a proper value to cause cancellation. The filtering operation to construct ATX from PTX can be also implemented in time domain; in which case only one IFFT block is used. The self-interference remaining in the base-band signal after analog active cancellation is a linear combination of PTX,

[3] [6]-[9] do not discuss antenna design and [10][11] rediscovered the same antenna structure as in Fig. 1 of the author's issued patent [2]

[4] Due to space limitations, refer to [1] for details.

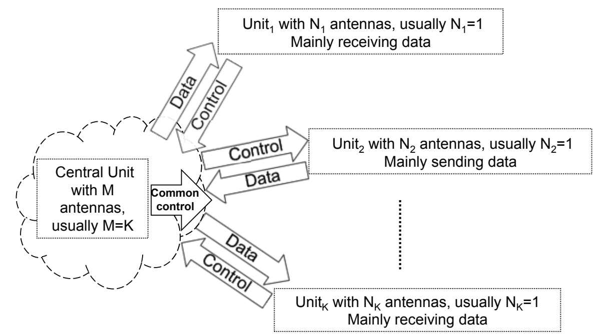

Fig. 1: $2K$ pipes of data/control are established over the same time/frequency where control includes reference for time/frequency/clock synchronization, channel gain/phase, information for user selection and channel inversion in SDMA, channel matrix in MIMO, ARQ, power control, instruction for adaptive coding and modulation, etc. In SDMA down-link, main data flow is out of central unit, while in SDMA uplink most data flow is into the central unit. Common control includes reference for time/frequency/clock synchronization.

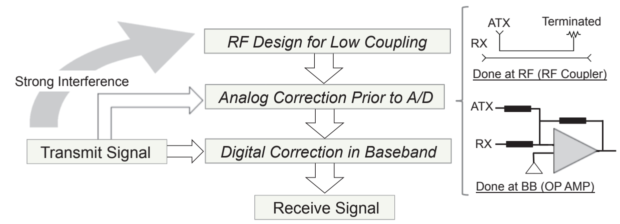

Fig. 2: Main components involved in self-interference cancellation.

ATX, which due to maintaining the linearity can be modeled as the PTX signal passed through a linear system. This linear system is measured through training and its OFDM structure is used to subtract the remaining self-interference in the digital domain.

Figures 2 and 3 illustrate abstract views of the system. PTX and ATX signals are pre-weighted in each OFDM tone such that they cancel each other at the RX chain. The weights are obtained by sending two separate (in time or frequency) pilots from PTX and ATX chains to measure the PTX to RX and ATX to RX base-band channels. These channels are denoted by H_1 and H_2, respectively. It is not possible to measure H_1 and H_2 accurately, as various imperfections, including additive noise, affect the accuracy of the measurement. Let ΔH_1 and ΔH_2 respectively denote the possible error terms in the measurement of H_1 and H_2. The weighting factors applied to TX and ATX are $(H_2 + \Delta H_2)$ and $-(H_1 + \Delta H_1)$, respectively.

ATX chain is designed to have a high coupling with the RX chain. This avoids the use of a Power Amplifier (PA) for the ATX chain and consequently helps to maintain linearity in the ATX path. In this case, the non-linearity of the PA in the PTX chain is modeled in time, using measurements in frequency domain. Due to the linearity of the ATX chain and the fact the PA non-linearity is invertible, one can construct a proper base-band ATX signal such that the overall effects of the PA non-linearity and the filtering operations due to H_1 and H_2 are compensated.

The remaining self-interference after analog active cancellation, referred to as residual self-interference RSI, is subsequently canceled digitally at the base-band. To this aim, the equivalent transmit to receive base-band channel (considering both TX and ATX chains) should be measured. The measurement is performed by sending two weighted pilots simultaneously as TX and ATX signals using the weights computed in the earlier phase. This second training phase results in the following signal in the base-

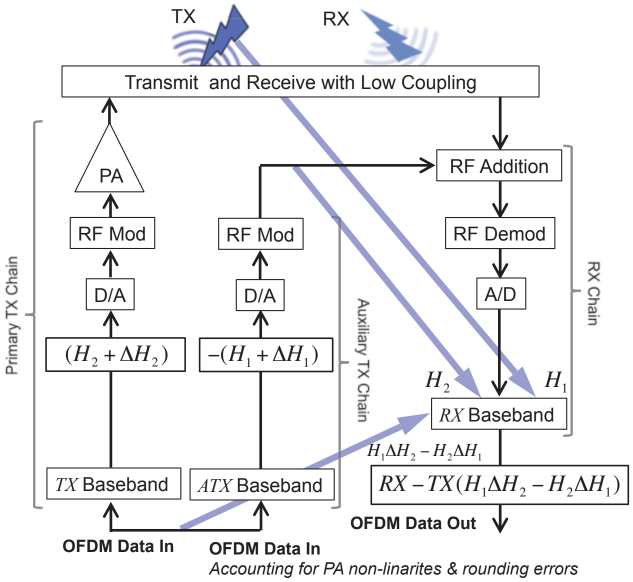

Fig. 3: Details of the self-interference cancellation.

band.

$$(H_1\Delta H_2 - H_2\Delta H_1)P + (H_1\Delta H_2 - H_2\Delta H_1)\Delta P \qquad (1)$$

where P and ΔP respectively denote the pilot signal and its possible error term. Assuming

$$(H_1\Delta H_2 - H_2\Delta H_1)\Delta P \approx 0, \qquad (2)$$

the equivalent transmit to receive base-band channel, denoted by H_E, is consequently obtained as

$$H_E = H_1\Delta H_2 - H_2\Delta H_1. \qquad (3)$$

Since H_E is of lower magnitude as compared to H_1 and H_2, it can be measured more precisely (in terms of relative error). The accuracy of the measurement of H_E can be also improved by repeating the measurement several times and averaging the values. Now, let us assume the OFDM data frame Γ, including a possible error term $\Delta\Gamma$ representing computational errors due to finite precision arithmetic, is passed through TX and ATX chains. The corresponding RI_{BB} at the receiver is:

$$RI_{BB} = H_E(\Gamma + \Delta\Gamma). \qquad (4)$$

The term $H_E\Gamma$ in (4) is digitally subtracted at the base-band. The term $H_E\Delta\Gamma$ is compensated digitally. Note that the above expressions symbolize the operations in order to explain the different terms and their effects. In practice, the error term due to imperfections in the D/A path, including numerical errors, is more sophisticated, and in particular depend on the method used for the actual implementation of filtering operations. In general, two factors contribute to such errors, namely "finite precision in intermediate computations", and "rounding effects to cast the result to the limited number of bits of D/A". Details of implementation are beyond the scope of this article, however, it is crucial to manage such errors as their effects in the final reconstructed signal, if not compensated, will be a noise with a power scaling with the power of self-interference.

Aside from the rounding effects (to limit the number of bits to what is supported by the D/A), the actual D/A conversion is a linear operation. As a result, channel measurements and subsequent computations in constructing the filters involved in active cancellation stage need not to be accurate. An error in these measurements will act as an additional parasitic linear system. As a result, the equivalent channel for the residual self-interference

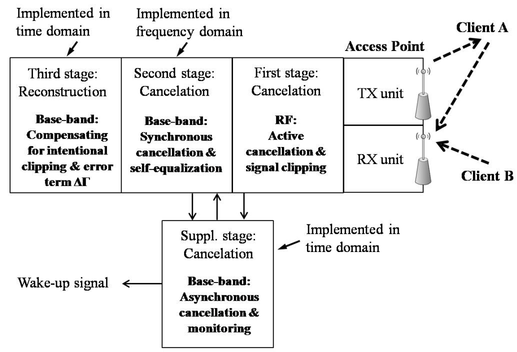

Fig. 4: Self-interference cancellation stages at an access point with a supplemental stage to support new clients in an asynchronous manner.

remains linear and can be handled relying on its OFDM structure. In other words, as long as H_E is measured accurately, the residual self-interference can be successfully compensated at the base-band. To measure H_1, transmit power of the training signal is reduced to keep the PA in linear regime. In practice, in the measurement of H_E, several training signals are averaged to reduce the effect of the measurement error. Note that Fig. 3 is just an abstraction aimed to represent various possibilities to realize the filtering operations. For example, for simplicity, only the ATX signal can be filtered in time domain, while filter coefficients (channels' impulse responses) are measured in the frequency domain. Another option is to apply separate filtering (in time) to PTX and ATX. Note that if the ATX chain has a direct coupling to the receive chain, the ATX will have a flat frequency response and consequently the filtering applied to PTX will not affect the magnitude of the OFDM tones aimed at distant users.

Although above derivations depend on the particular method used for filtering, the general argument that the first order approximation of the remaining self-interference forms a linear channel, which can be measured to be used in digital cancellation, applies to a wider class of implementations. Note that unlike the first stage of analog cancellation, the energy of the remaining self-interference (to be digitally cancelled in the second stage) is comparable to that of the signal received from distant user and consequently the error due to using a first order approximation, such as shown in Eq. 2, can be ignored.

To handle asynchronous users, the access point continually monitors its incoming signal to detect a valid request-to-join signal from a new client while supporting full-duplex connections to its current clients. Several periods of a periodic sequence are commonly used as a request-to-join signal in practical systems. When such a signal passes through the linear system corresponding to the channel between the access point and the new client, it results in an almost periodic sequence of the same period. In order to detect this periodic signal, a supplemental stage of interference cancellation is performed in time domain at the base-band. This stage operates asynchronously and in parallel with the main base-band interference cancellation stage that is implemented in frequency domain (see Fig. 4). This supplemental stage of cancellation does not require to completely cancel the self-interference. It is sufficient to reduce the amount of self-interference to the level that the aforementioned periodic signal is detectable. The output of this stage informs the access point that a new user requests to join the network. The access point then allocates resources to this user and synchronizes it with the current users within the cyclic prefix of the underlying OFDM scheme.

III. Antenna Design

A full-duplex node can be considered as a two-port network described in terms of scattering parameters S_{11}, S_{12}, S_{21}, and

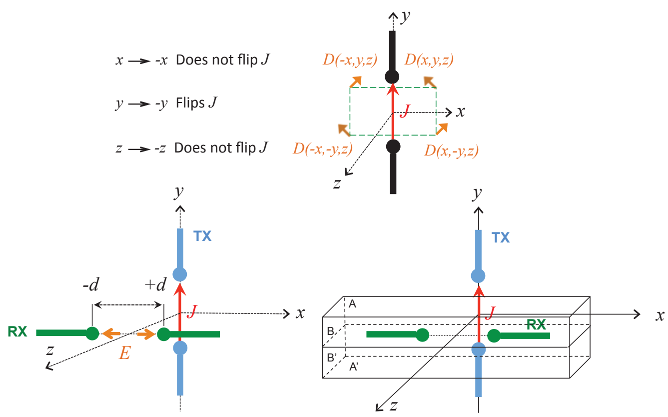

Fig. 5: Par-wise symmetrical antennas with input current (I) in the y-axis direction. Net energy flowing out the whole region around the RX antenna is zero which results in $S_{12} = S_{21} = 0$.

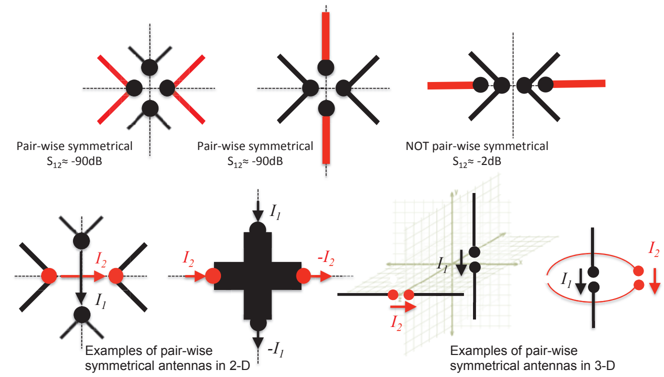

Fig. 6: All structures are pair-wise symmetric except for the one on top right corner which shows significant coupling.

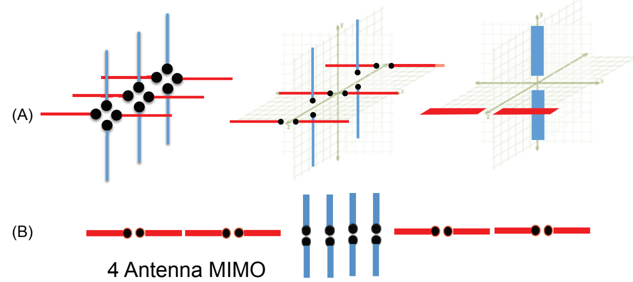

Fig. 7: Two and Three-dimensional antennas for MIMO structure.

S_{22}. The objective is to reduce coupling between TX and RX chains, i.e., $S_{12} = S_{21}$ should be small. It is also desirable to have small S_{11} and S_{22} for better antenna efficiency. Moreover, the above conditions should be satisfied over the entire operating frequency range. Note that the low coupling requirement in a full-duplex node is different from that of MIMO systems. In MIMO, it is desirable that the channels between transmit and receive antennas in distant nodes are independent. This is achieved by spacing the antennas sufficiently far apart. For low coupling in a full-duplex node, however, transmit and receive antennas within the same node should induce small power on each other. Using techniques proposed in this section, such antennas can be placed close to each other while having a small coupling over the desired frequency band. Due to vicinity of transmit and receive antennas, near-field effects will be significant and dominate the system behavior. This feature is indeed beneficial.

According to Maxwell equations, geometrical symmetry in structure (shape, material, boundary conditions) and excitation (feed terminals) of an antenna lead to geometrical symmetry in electric and magnetic fields. The geometrical symmetry in antenna fields can be used to cancel the self-interference. The following definitions are useful in subsequent theorems.

Definition 1: An antenna is called *self symmetric* if its two arms are image of each other with respect to a plane of symmetry. This includes the symmetry of construction, excitation, and parasitic elements.

Definition 2: Two antennas are called *pair-wise symmetric* if the following conditions are satisfied: (i) each antenna is self symmetric; (ii) the two antennas have different planes of symmetry; (iii) each antenna is invariant under reflection in the plane of symmetry of the other one.

The following two theorems follow (see [1] for proof).

Theorem 1: For a self symmetric antenna, electric and magnetic fields are invariant under a symmetry which does not change the direction of the antenna's input current, and are invariant with sign change under a symmetry which changes the direction of the antenna's input current.

Theorem 2: If the transmit and receive antennas of a full-duplex node are pair-wise symmetric, then they have zero coupling, i.e., $S_{12} = S_{21} = 0$ independent of frequency.

In practice $S_{12} = S_{21}$ is close to zero (e.g., -40 to -70 dB) due to reflections from surrounding environment, and sources of imperfections in hardware realization. In our design, we have aimed to maintain the symmetry in the entire circuit structure. Low coupling in RF is crucial. It should bring any remaining residues in the analog cancellation to a level below the Gaussian noise. Otherwise, as such residues will be amplified by the LNA, they will raise the effective noise level. This feature is one of the main reasons for the superior performance as compared to other implementations [3]-[11].

Fig. 6 illustrates some examples of pair-wise symmetric antennas. Figure 6 also shows that the coupling between antennas can be very strong ($S_{12} = -2$ dB) due to the near-field effect unless it is canceled relying on pair-wise symmetry. The values of coupling are obtained by using high frequency structural simulator (HFSS) at 2.4 GHz band.

The idea of symmetry is generalized to obtain triple-wise symmetric antennas in three dimensions in Fig. 7(A). Note that pair-wise symmetric structures require two dimensions effectively, and as a result, it is possible to generate more transmit/receive antennas along the third dimension. As a result, MIMO structures with zero coupling can be realized in three dimensions. Fig. 7(A) shows an example where every antenna in TX set (say antennas parallel with the x-axis) is decoupled from all the antennas in RX set (antennas parallel with the y-axis). Three-dimensional antennas with pair-wise symmetry can be implemented by using opposite sides or different layers of a PCB. Figure 8 shows a MIMO configuration in which antenna arms are merged into a single patch above the ground plane. ATX coupling is achieved using a third terminal for the same patch (with a high coupling to the RX terminal). Figure 8 shows a MIMO configuration using several of such three terminal patch antennas, while satisfying the triple-wise symmetry condition. As an alternative to realize MIMO (with low, but nonzero coupling), one set of antennas can be placed along the plane of symmetry of the other set. Since electric field of a self-symmetric antenna is orthogonal to its plane of symmetry (bisecting its feed terminals), this configuration results in low coupling. Figure 7(B) shows a 4×4 arrangement. Shape of arms and spacing between antennas can be adjusted to compensate for lack of perfect symmetry, and for non-zero width of antennas' arms. Fig. 9 shows that the coupling between two antennas can be improved from -70 dB to -110 dB by modifying shape of arms. Results are obtained at 2.4 GHz band using HFSS.

Fig. 8: Pair-wise symmetry in 2.5 D with generalization to MIMO.

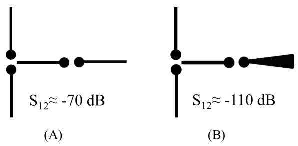

Fig. 9: Shape of arms is adjusted to compensate the lack of symmetry in a low coupling structure.

IV. Applications

Security: Two-way links are inherently more secure as Eve receives a combination of Alice's and Bob's signals [12] [13]. To further enhance security, after the initial connection is established, Alice can use the return link to randomize the forward transmission, e.g., by introducing random offsets in carrier frequency for every new block of OFDM symbols.

Two-way connectivity enables increasing the number of transmit antennas to improve SNR by facilitating the training phase. This feature can be used as a tool in improving throughput, or to make eavesdropping difficult by improving the SNR of the legitimate link (see Fig. 12 where the two sets switch between transmit & training/receive modes in subsequent blocks).

Two-way connectivity also provides the ground for a novel method to achieve unconditional security (see [1] for further details). This is based on using full-duplex capability to form a close loop between legitimate units. The phase of this loop is measured and used as a key to mask a PSK transmission, which contains bits of a binary key. Several realizations of such a setup are discussed in [1], and one case is shown in Figs. 13 to 16.

Networking: Synchronization is a major bottleneck in the realization of network information theoretic setups. Relying on two-way links, one node can broadcast a set of pilots to be used by all network nodes as reference. In down-link SDMA, the return channels can be used to feedback channel state information, or in up-link SDMA, central node can broadcast control signals to synchronize all the clients, or inform them how to rotate/scale their respective constellations to facilitate joint or successive detection. Two neighboring nodes, by listening to each other while transmitting, can form a distributed Alamouti code. Another application is in interference channel, in which each node can filter/amplify/forward the signal received from the other node to cancel the interference coming through the cross links (see Fig. 10). In addition, the feedback link is useful in sending pilots, in Automatic Repeat-reQuest (ARQ), in adaptive transmission, etc., or nodes can have an indication of the level of interference by listening while transmitting. In cognitive setups, the possibility of listening while transmitting enables the secondary users to enjoy the free channel and stop their transmission immediately upon receiving the preamble (used as a signature) of the primary users, and continuing when once again channel is free of licensed users. Possibility of supporting two-way asynchronous links with multiple clients solves many of resource allocation scheduling issues in wireless networks. A major bottleneck is to establish control signaling, particularly signaling in uplink required to join the network. In current half-duplex networks, data and control links are established either using different frequency bands, or using different time slots. Solutions based on frequency division duplex are expensive, and solutions based on time division duplex are usually inefficient. Full-duplex connectivity enables

	uWaterloo	Rice	Stanford
Working in environments with strong reflection	Yes	No	No
RF isolation through antenna design	Yes (with much improvements vs. author's 2010 patent)	No	Yes (but uses same structure as in author's 2010 patent)
Super Analog Active: Active Cancellation exploiting linearity of D/A	Yes	No	No
Methods to deal with phase noise and non-linarites	Yes	No	No
Applications of two-way	Yes	No	No

TABLE I: Summary of comparison with Rice [6]-[9] and Stanford teams [10] [11].

superimposing (physical overlay) a network of low throughout, low power control links on top of the network of High Througput Data (HTD) links. Transmission on the Low Throughput Overlay (LTO) channel is of low power and low spectral efficiency, separated from the HTD links in the code domain. Nodes involved in signaling over HTD channel can first search for the LTO signal, perform signal detection on it, and then cancel it prior to the detection of HTD channel. Methods proposed for handing asynchronous clients provide the framework to implement a network of LTO links working asynchronous and in parallel with the network of HTD links without causing noticeable degradation (see Fig. 11 and [1] for further details).

References

[1] A. K. Khandani, on line (video) presentation of two-way wireless posted April 2012. www.cst.uwaterloo.ca

[2] A. K. Khandani, "Methods for spatial multiplexing of wireless two-way channels," US Patent number: 7817641, Filing date: Oct 17, 2006, Issue date: Oct 19, 2010, Application number: 11/581,427

[3] K. Tsubouchi, H. Nakase, A. Namba, K. Masu, Full duplex transmission operation of a 2.45-GHz asynchronous spread spectrum using a SAW convolver, IEEE Transactions on Ultrasonics, Ferroelectrics and Frequency Control, Sept. 1993 (Res. Inst. of Electr. Commun., Tohoku Univ., Japan)

[4] S. Chen, M. A. Beach, J.P. McGeehan, Division-free duplex for wireless applications, Electronics Letters, Jan. 1998, (Centre for Commun. Res., Bristol Univ.)

[5] B. Radunovic, D. Gunawardena, P. Key, A. Proutiere, N. Singh, V. Balan, G. Dejean, Rethinking Indoor Wireless: Low Power, Low Frequency, Full-duplex, "Microsoft Technical Report MSR-TR-2009-148", July 2009

[6] M. Duarte and A. Sabharwal, Full-Duplex Wireless Communications Using Off-The-Shelf Radios: Feasibility and First Results, Asilomar Conference on Signals, Systems, and Computers, Nov. 2010

[7] A. Sahai, G. Patel and A. Sabharwal, "Pushing the Limits of Full-duplex: Design and Real-time Implementation", Rice tech report, Feb. 2011, see also announcements by Rice University (Sept. 2011): http://www.youtube.com/watch?v=tXMwn2mm0VY

[8] M. Duarte, C. Dick and A. Sabharwal, "Experimental-driven Characterization of, Full-Duplex Wireless Systems", submitted to IEEE Transactions on Wireless Communications, June 2011

[9] E. Everett, M. Duarte, C. Dick, and A. Sabharwal, "Exploiting Directional Diversity in Full-duplex Communication, Asilomar Conference, Nov. 2011

[10] J. Choiy, M. Jainy, K. Srinivasany, P. Levis, S. Katti, "Achieving Single Channel, Full Duplex Wireless Communication," Mobicom 2010, Sept. 2010. See also announcement by Stanford University (Feb. 2011): http://www.youtube.com/watch?v=RiQb5NdDWgk

[11] M. Jain, J. Choi, T. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, P. Sinha, "Practical, Real-time, Full-Duplex Wireless", Mobicom, Sept. 2011

[12] Lifeng Lai, El Gamal, H. ; Poor, H.V. "The Wiretap Channel With Feedback: Encryption Over the Channel," *IEEE Transactions on Theory*, Volume: 54 , Issue: 11, Page(s): 5059-5067

[13] El Gamal, A., Koyluoglu, O.O. ; Youssef, M. ; El Gamal, H., "New achievable secrecy rate regions for the two way wiretap channel", *2010 IEEE Theory Workshop (ITW)*, 6-8 Jan. 2010, Page(s): 1-5

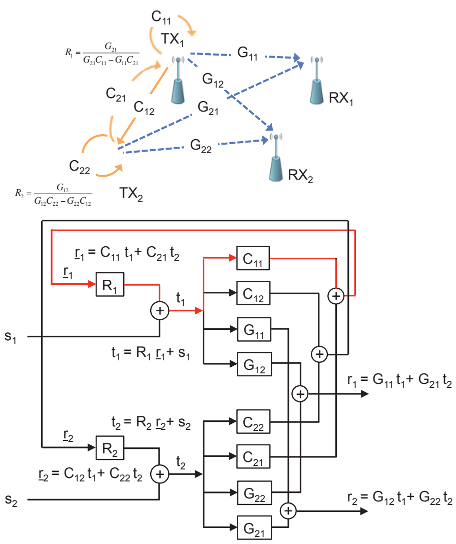

Fig. 10: R_1 and R_2 are filters at receivers of nodes TX1 and TX2, respectively. These filters superimpose a signal on the direct path which will cancel the interference from the cross links. Stability condition is satisfied by adjusting TX/RX gains.

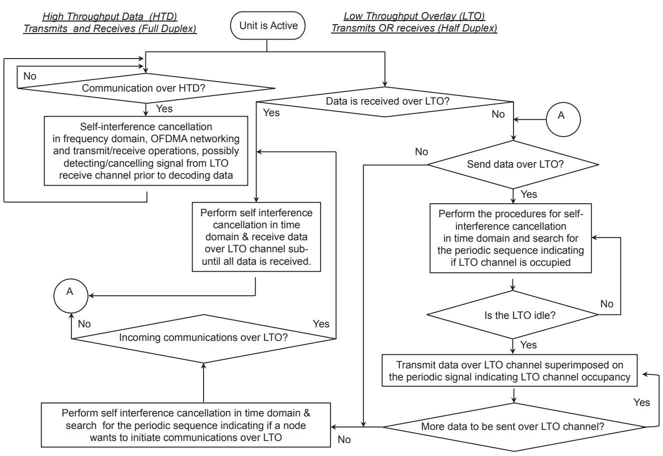

Fig. 11: Flow chart for superimposed networking.

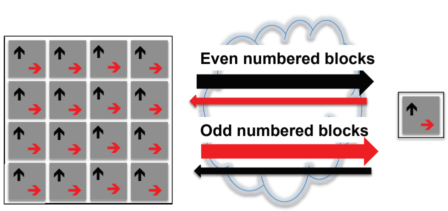

Fig. 12: Use of many antennas towards improving SNR.

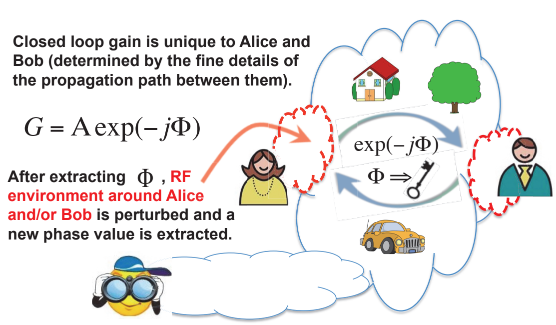

Fig. 13: Key exchange in unconditional security.

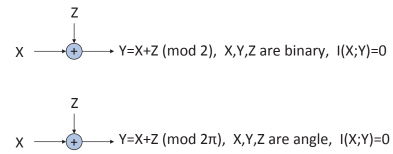

Fig. 14: Masking through modulo addition of phase values for unconditional security. Phase masks are obtained through measuring the channel between the legitimate parties at both ends. The number of transmissions to perform this measurement is limited and is done in a manner that eavesdropper encounters one unknown phase corresponding to each of its receive antennas (phase between eavesdropper receive antenna and antenna of the legitimate transmitter). Each shared phase value will be used to mask a PSK transmission, containing some of the bits of the final key. Errors between the measured phase values at the two legitimate parties will be part of errors observed in traditional systems and will be corrected by the underlying error correcting code.

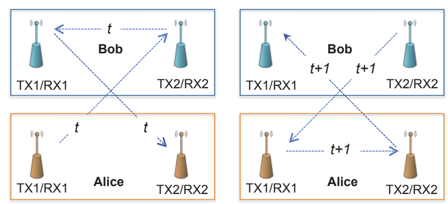

Fig. 15: Steps in key exchange: 1- At time $t-1$, Alice and Bob measure their loop-back channels from Bob/TX1 to Bob/RX2 and from Alice/TX2 to Alice/RX1 (send low power pilots after scrambling and loop back in each unit). 2- At time t, Alice/TX1 sends pilots (after scrambling) to Bob/RX2, who (using Bob/TX1) forwards it to Alice/RX2. 3- At time $t+1$, Bob/TX2 sends pilots (after scrambling) to Alice/RX1, who (using Alice/TX2) forwards it to Bob/RX1. 4- The two units, knowing their loop-back channels and relying on reciprocity, compute the channel:(Alice/TX1 to Bob/RX2)x(Bob-loop-back)x(Bob/TX1 to Alice/RX2)x(Alice-loop-back) to be used a key. This is possible as up/down conversion at each unit is performed using the same carrier/clock.

.

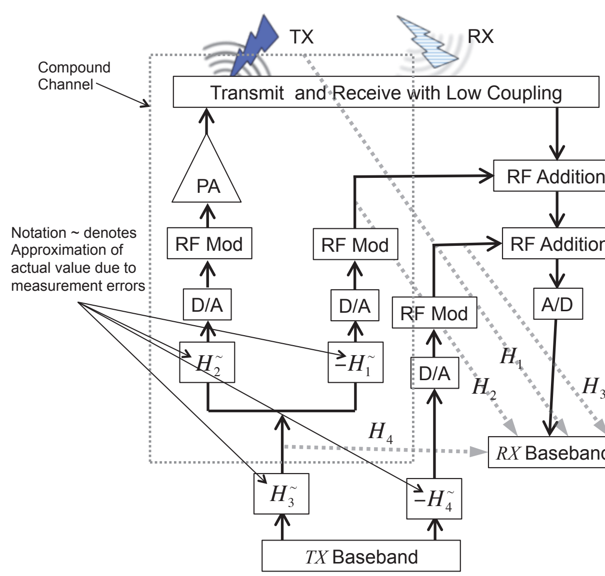

Fig. 16: Block diagram for cascade of analog cancellation. This enhances the ability for cancellation of self-interference through time domain filtering, and consequently, can be used to avoid delay (typical of OFDM) in closing the loop between legitimate parties in a key exchange protocol.