Secrecy Rate Based User Selection Algorithms for Massive MIMO Wireless Networks

M. Arif Khan(✉) and Rafiqul Islam

School of Computing and Mathematics, Charles Sturt University,
Bathurst, NSW 2678, Australia
{mkhan,mislam}@csu.edu.au

Abstract. In this paper, we investigate user selection algorithms for massive MIMO downlink wireless channel using secrecy rates. Massive MIMO is new disruptive wireless communication technology that exploits the benefits of having large number of antennas at the base station (BS). Given the fact of large antenna dimensions at BS, still the number of devices/users in the system are larger than total antennas. Hence, selection of an optimal set of devices/users for efficient resource allocation is a critical issue. This paper investigates user selection algorithms in massive MIMO downlink/broadcast wireless system. Traditional selection algorithms are generally based on channel strength, channel angle information, algorithm complexity and capacity maximization. In this paper, we investigate selection algorithms based on secrecy rate which is important parameter for secure transmission and compare the performance of this new approach with existing algorithms.

Keywords: Conventional MIMO · Massive MIMO · Secure transmission · User selection · Secrecy rate · Active attack

1 Introduction

Security in any wireless communication is an utmost important issue due to the nature of wireless transmission. At the application layers, security is achieved through encrypting data before transmission. In most of the wireless networks, it is assumed that encrypting data at the application layer inherently incorporates the physical layer security as well. However, such encryption techniques do not consider the challenges and problems at the physical layer implementation. In [1], authors showed that using large number of antennas in a communication system makes it more robust and protective against passive eavesdropping attacks. It is also shown that with massive MIMO and passive eavesdropper, the situation of physical layer security (PLS) changes dramatically. This enhanced security is due to the fact that in conventional MIMO, the two rates of a legitimate device and an eavesdropper are of similar order of magnitude, whereas in massive MIMO these two rates have a considerable difference and hence the secrecy rate becomes an important measure. Massive MIMO also provides an advantage that

B. Thuraisingham et al. (Eds.): SecureComm 2015, LNICST 164, pp. 697–710, 2015.
DOI: 10.1007/978-3-319-28865-9_46

wireless channels of different devices/users are almost orthogonal to each other that helps the BS to align and beamform transmission signals to intended users more efficiently.

Massive MIMO is one of the major disruptive technologies for next generation 5G wireless networks where huge amount of devices will communicate with each other via internet [17]. Authors of [17] proposed that massive MIMO can be used to multiplex signals from several devices on each time-frequency resource and can be beamformed towards the intended users while minimizing the interference for other devices. It is anticipated that with a large number of devices communicating simultaneously; security, privacy and data integrity will become critical issues in designing future generation wireless networks. Authors of [18], present a new concept of embedded security at the physical layer by realizing that current security solutions fall short in terms of scalability with sheer number of devices connected in 5G systems. Their proposal is to exploit the reciprocity and fading of wireless channel information and to establish a common secret code between sender and transmitter from the channel information measurements. This information will not be accessible / decodable by the eavesdropper.

So the challenging task here is that when there are large number of devices contending for the resource from base stations, how to schedule a proper set of devices such that information to them can be transmitted securely? In massive MIMO system we have large number of antennas at the BS compared to conventional MIMO systems. Therefore, this new system can accommodate a large number of devices simultaneously. However, with the introduction of new wireless paradigms, such as Internet of Things (IoT), where each device is connected to the other device and access point (BS), proper device scheduling within given resources is an important issue. In conventional MIMO, efficient selection and scheduling of devices play a key role in the system throughput [9, 10, 11, 15]. However, in massive MIMO the research area of efficient and secure selection of devices is yet not fully explored. In this paper, we focus our attention to the problem of device selection and secure transmission of the information. We first discuss some already existing device selection algorithms for conventional MIMO that we can extend to massive MIMO systems. Then we propose a new device selection algorithm based on secrecy rate that can make sure that the information can be transmitted securely since it satisfies the condition of secrecy rate. Each device calculates its channel information and sends it back to the base station through an error free and minimum delay feedback channel. The base station calculates the secrecy rate for each device knowing that there is an eavesdropper and also knowing its channel information. BS then selects only those devices having data rates higher than the secrecy rate making sure that signal transmitted for a device is beamformed in its direction and the leakage signal towards eavesdropper is minimum. This algorithm performs reasonably well compared to other existing algorithms.

Rest of the paper is organized as follows. Section 2 describes Multiple Input Multiple Output (MIMO) systems. In this section, we describe both conventional and massive MIMO systems in detail. Section 3 presents system and wireless

channel model used in this paper. Section 4 discusses user selection algorithms. In this section, we present both traditional and secrecy rate based user selection algorithms. Section 5 presents simulation results and discussion on the results. Finally, in Section 6 we conclude the paper.

2 Multiple Input Multiple Output (MIMO) Systems

In this section we introduce and discuss multi-user MIMO systems. Although, MIMO technologies are being used in the current wireless networks, its new and advance versions are still being introduced. We will highlight the importance and advantages of MIMO in wireless communication systems. We will also discuss conventional and massive MIMO and present the main differences in the two different yet similar technologies.

2.1 Conventional MIMO

In conventional MIMO systems, range of BS antennas, generally, is assumed between 2 to 8. Such MIMO systems promise high system throughput without increasing the transmit power or using large bandwidth since both are scarce resources. With the emergence of MIMO technology in mid 1990s, there has been a lot of interest in MIMO systems research and now is being used in most of the contemporary wireless communications. In addition to conventional time and frequency dimensions, MIMO leverages the benefits of spatial dimension [8, 9, 10, 11]. A typical conventional multi-user MIMO communication system is shown in Figure 1.

Efficient resource allocation and user selection is one of the important research areas of MIMO wireless systems. With the introduction of various new applications in wireless communication systems, the number of users (devices) has been increased exponentially as well. It became difficult for MIMO systems to serve all of these mobile devices / users simultaneously. Besides this, some users / devices / applications demand different resources than others. This has made user selection problem a trivial problem to solve for MIMO systems. In conventional MIMO, a number of researchers proposed user selection and scheduling algorithms based on various criterion such as channel strength, angle of separation among users, rate supported and complexity [9, 10, 11] few to name. We will further discuss different user selection algorithms in Section 4 of the paper.

2.2 Conventional MIMO Security Model

In conventional MIMO systems, secrecy capacity is defined as the system capacity that promises the integrity and confidentiality of the transmitted data. Most common MIMO security model is known as wiretap channel model where a transmitter sends some legitimate confidential information to one user for which it is intended whereas the other user is an eavesdropper [12]. In this paper, our discussion provides an insight on user (device) selection algorithms based on the

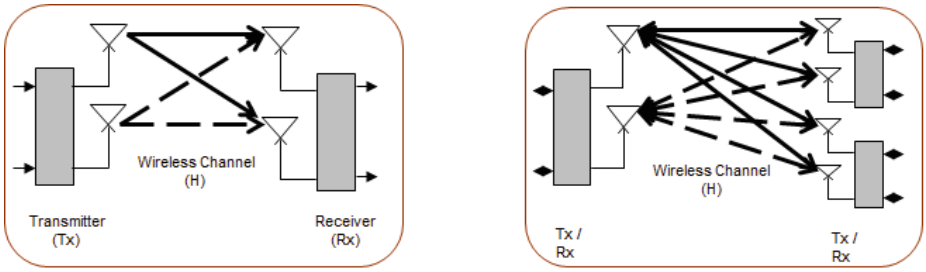

Fig. 1. A typical single user (left) and multi user (right) conventional MIMO wireless communication system.

secrecy rate that guarantees the promised data rate for intended user and makes the rate zero for an eavesdropper. The security model for a received signal, y_k, using MIMO system can be written as follows:

$$y_k = \mathbf{h}_k \mathbf{w}_k (\mathbf{s}_k + \mathbf{a}_k) + \sum_{j=1, j \neq k}^{M} \mathbf{h}_j \mathbf{w}_j (\mathbf{s}_j + \mathbf{a}_j) + n_k, \tag{1}$$

where $\mathbf{a}_k$ represents the attack vector from a non-legitimate user. It is worth noting that secrecy rate in conventional MIMO model is of similar magnitude as that of other rates, making it difficult to select an efficient user subset.

2.3 Massive MIMO

In massive MIMO (or large-scale MIMO) systems, number of antennas at the base station is in the range of hundred or more. This new MIMO paradigm has recently been proposed by *T. L. Marzetta* in his paper cited as [4] and later on many others such as [5, 6]. There has been a lot of interest in massive MIMO from academic and industrial communities. This is due to the reasons that massive MIMO potentially can fulfill the demand of big data services and the high bandwidth requirements in emerging Internet of Things (IoT) technologies. The author in [4] presented a multi-user MIMO system with an infinite number of base station antennas in a multi-cellular environment. We refer such a MIMO system as massive MIMO system here. In [6], authors discussed the potential advantages of massive MIMO system and highlighted that with the availability of large Degrees of Freedom (DoF), hardware-friendly signal shaping can be achieved for the better system performance. With the introduction of many signal streams in massive MIMO systems, security challenges grow as well. The system needs to integrate more efficient and effective encryption before transmitting the data to intended users.

3 System and Transmission Model

In this section, we present system and transmission model. We consider a single cell multiuser massive MIMO downlink (from BS to users) where base station (BS) transmits signals to multiple mobile terminals (MT) simultaneously as shown in Figure 2. These MTs can be either hand held devices or any other mobile device with the wireless communication capability. Let us assume that the BS has M transmit antennas and there are K number of MTs where each MT has a single receive antenna. This system model can easily be extended to MTs with multiple receive antennas, but for the sake of simplicity we assume MTs with a single receive antenna in this paper. Let us consider that the BS transmits a confidential data signal s_k to the k^{th} MT. We can then denote the signal vector to all K MTs by $\mathbf{s}$ which is given as $\mathbf{s} = [s_1, s_2, \cdots, s_K]^T \in C^{(K\times 1)}$ where each signal vector is precoded using a beamforming matrix, $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_K] \in C^{(M\times K)}$ before transmission. Let us assume the total transmit power to be P and there is equal transmit power allocated to each MT, denoted by p and defined as $p = P/K$. Then the received signal at k^{th} MT denoted by y_k and at the eavesdropper denoted by $\mathbf{y}_e$ is given by:

$$y_k = \sqrt{p}\mathbf{h}_k\mathbf{w}_k s_k + \sum_{j=1, j\neq k}^{K} \sqrt{p}\mathbf{h}_j\mathbf{w}_j + n_k, \tag{2}$$

and

$$\mathbf{y}_e = \sqrt{p}\mathbf{H}\mathbf{W}\mathbf{s} + \mathbf{n}_e, \tag{3}$$

where $\mathbf{h}_k \in C^{1\times M}$ represents the wireless channel vector of the k^{th} MT with its elements being complex Gaussian random variables with zero mean and unit variance. Let us denote the rate of k^{th} MT by R_k and is given as follows:

$$R_k = \log_2 \det\left(\mathbf{I}_M + p\mathbf{w}_k\mathbf{h}_k\mathbf{h}_k^H\mathbf{w}_k^H\right), \tag{4}$$

where $(.)^H$ represents Hermitian operator. Similarly, the capacity of an eavesdropper represented by C_e is given as follows:

$$C_e = \log_2 \det\left(\mathbf{I}_M + p\mathbf{w}_k\mathbf{h}_e\mathbf{h}_e^H\mathbf{w}_k^H\right). \tag{5}$$

Before transmission of the signal, it has to be precoded at the BS in order to minimize the interference for other users and also preventing for an eavesdropper. In conventional MIMO systems, typically Zero Forcing (ZF) and Minimum Mean Square Error (MMSE) based precoding schemes are used. However, due to huge computational complexity of these schemes for large dimensional arrays, typically of complexity order as $O(L^3)$ where L is the array size [13], we adopt the precoding approaches of simple ZF and conjugate beamforming (CB) as discussed in [19]. Therefore, the precoding vector for each user using ZF beamforming can be calculated as $\mathbf{w}_k = \mathbf{h}_k^H/||\mathbf{h}_k||$.

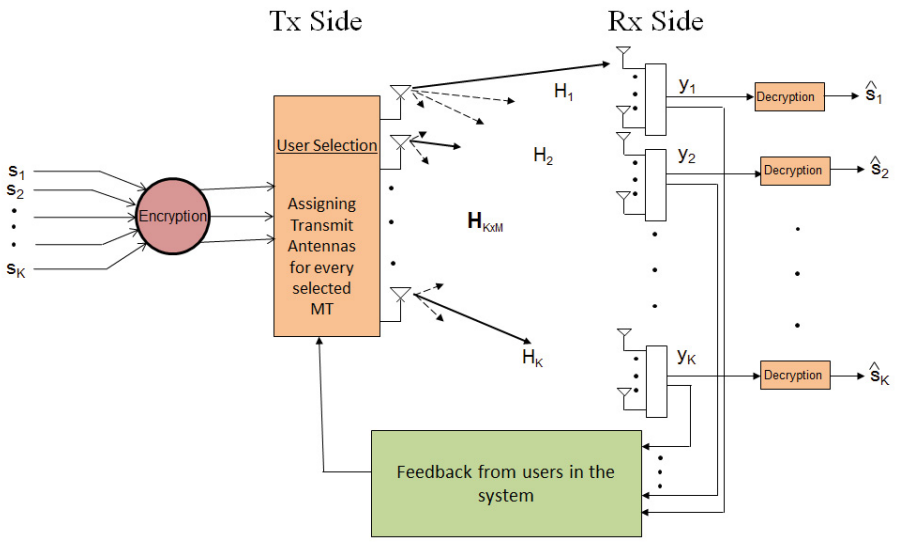

Fig. 2. Massive MIMO downlink / broadcast system used in this paper.

3.1 Feedback Model

In MIMO broadcast system, BS selects a set of devices based on certain information that it receives from devices. In most of the cases, this information is relevant to the wireless channel condition of the device. BS transmits a pilot signal for all active MTs in its vicinity. All MTs receive this pilot signal and send the information back to the BS via an error free low time delay feedback channel. It is assumed in the system model that this feedback has no error and eavesdropper or adversary user cannot tamper this information. However, this assumption may not be very realistic since active eavesdroppers can access this information and then can modify it to benefit the wireless transmission in their own favor. However, for the sake of simplicity, we assume that this feedback is error free and attackers cannot access this information. BS then uses this feedback in the selection process. We refer this channel information as the Channel State Information at Transmitter (CSIT) in the remaining paper. The feedback path is shown in Figure 2.

4 User Selection Algorithms

Although in massive MIMO systems, number of antennas at the BS are very large, we still consider that total number of users in the system are larger than total number of antennas at the BS. Therefore, BS needs to select a subset of users from all active users for transmission. Let us assume that the BS selects a subset S of users from K total active users such that $S \geq K$. BS then precodes

the signals of these selected users before transmission by using the precoding matrix $\mathbf{W}$. There are a large number of user selection schemes available in conventional MIMO systems that can be used in massive MIMO systems as well. However, in this paper we discuss only three existing schemes. Our contributions in this paper are to extend these techniques from conventional MIMO to massive MIMO while considering the secure transmission in the selection process. Also we present a new user selection technique that is based on secrecy rate and we compare its performance with other existing schemes. In particular, user selection schemes that we present in this paper are: (i) Exhaustive Search (ES), (ii) Frobenius Norm based Selection (FNS), (iii) Round Robin Selection (RRS), and (iv) Secrecy Rate based Selection (SRS). The user selection techniques generally introduce extra computational complexity in the system, but on the other hand they also maximize the system performance which is essential for securing the data transmission at physical layer. Among all user selection techniques, ES is the best and optimal selection technique as discussed in Section 4.1. ES guarantees the maximum achievable system throughput, however, it also has very high search complexity. Also its search domain increases exponentially with the increase of users in the system. Therefore in practical systems, where number of users is generally very large, ES cannot be implemented. For example, in our system model we are required to select S users out of total K users with M number of antennas at the BS in such a way that for each user the secrecy rate condition is satisfied. Then the search domain for BS using ES selection technique becomes as follows:

$$D_S = \binom{K}{S} = \frac{K!}{S! \times (K-S)!} \tag{6}$$

Example: Let us consider that we have a conventional MIMO system where BS performs the user selection. We are interested to calculate the search complexity in this system for the BS. Let us assume that there are $K = 50$ active devices in the system and the BS has $M = 10$ antennas so that is why it can possibly select $S = 10$ maximum devices for transmission simultaneously. This is a common scenario in most of the current wireless communication systems. Then the search domain for this selection process using ES with Equation (6) will become as 1.0272×10^{10} combinations which is very large considering the real time communication scenario. Therefore, it is important that we find such selection schemes that have low complexity for practical considerations, yet provide an acceptable system performance. In the following we discuss each device/user selection scheme.

4.1 Exhaustive Selection (ES)

In general Exhaustive Selection (ES) process computes all possible combinations therefore it has the largest search space; as a result its complexity grows exponentially with the linear increase in dimensions. ES in particular is not suitable for massive MIMO systems with large number of devices in the system. But on

Table 1. FNS based selection algorithm

Initialization: $S = \emptyset$, BS transmits pilot signal.
Step 1: Let $\mathbf{H} \in C^{K \times M}$ be the channel matrix of all active MTs and is defined as $\mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_K]$ where $\mathbf{h}_k \in C^{1 \times M}$ is the channel vector of the k^{th} MT and $k = 1, 2, \cdots, K$.
Step 2: Compute $\|\mathbf{h}\|_F^2$ using Equation (7) for each MT.
Step 3: Each MT sends its $\|\mathbf{h}\|_F^2$ value as a scalar feedback to the BS using error free feedback channel as shown in Figure 2.
Step 4: BS orders all received $\|\mathbf{h}\|_F^2$ such that $\left\|\overline{\mathbf{h}}_1\right\|_F^2 > \left\|\overline{\mathbf{h}}_2\right\|_F^2 > \cdots, \left\|\overline{\mathbf{h}}_K\right\|_F^2$ where $\overline{\mathbf{h}}_k = \left\|\overline{\mathbf{h}}_K\right\|_F^2$ represents the ordered values.
Step 5: Construct at the BS: $\overline{\mathbf{H}} = [\overline{\mathbf{h}}_1, \overline{\mathbf{h}}_2, \cdots, \overline{\mathbf{h}}_K]$.
Step 6: Select S MTs from $\overline{\mathbf{H}}$ such that $S = \{m_1, m_2, \cdots, m_S\}$ is the set of MTs for transmission.
Step 7: Calculate the precoding matrix for S selected MTs such that $\overline{\mathbf{W}} = [\overline{\mathbf{w}}_1, \overline{\mathbf{w}}_2, \cdots, \overline{\mathbf{w}}_S]$ where $\overline{\mathbf{w}}_k = \frac{\overline{\mathbf{h}}_k^H}{\|\overline{\mathbf{h}}_k\|}$.
Step 8: Calculate the rates of transmission for S MTs using Equation (4).
Step 9: Terminate the algorithm.

the other hand it is an optimal selection scheme in the context of maximizing the system throughput. In this paper, we use ES only to benchmark the other schemes since this is the maximum throughput that can be achieved in a multi user / device MIMO communication system.

4.2 Frobenius Norm Based Selection (FNS)

In Frobenius Norm based Selection (FNS), each MT on receiving the pilot signal from BS, calculates the squared Frobenius norm of its wireless channel $\mathbf{h}$ with dimensions $1 \times M$ as follows [14]:

$$\|\mathbf{h}\|_F^2 = (\mathbf{h}^H \mathbf{h}). \tag{7}$$

Different variants of FNS algorithm are available in MIMO literature such as [9, 10, 15] few to mention here. FNS is attractive in practical implementations since it requires only scalar feedback to be transmitted back to the base station. In a large device regime, such as IoT, this algorithm can be a favorable choice. The complete FNS algorithm implemented at BS is given in Table 1.

4.3 Round Robin Selection (RRS)

Round Robin Selection (RRS) is the simplest and the fairest selection technique which does not require CSIT. In this technique a subset or group of MTs is selected with equal probability. In a single MT case, required transmit/ receive

antennas are selected from total antennas randomly and the channel capacity is based on these selected antennas. In multi MTs, however, the subset of required MTs is selected randomly. The sum capacity of the system is based on these selected devices. The selection probability is kept uniform, so as to eliminate the fairness problem completely. The performance of this approach is very poor and it only sets the lower limit for performance. It has least computational complexity and also does not cause fairness problem but on the other hand results in the lowest sum capacity.

4.4 Secrecy Rate Based Selection (SRS)

In this selection algorithm, we make sure that a user / device receives guaranteed rate for transmission. In this proposed scheme, the BS selects a subset of devices in such a way that the secrecy rates of the selected MTs are greater than zero. A similar user selection algorithm for conventional MIMO downlink system is presented in [16]. Our proposed algorithm is different from the algorithm presented in [16] that it is for massive MIMO downlink systems and it is based on the selection process given in the following criteria [7].

$$R_k^{sec} = [R_k - C_e]^+ \tag{8}$$

where $[x]^+ = max\{0, x\}$, R_k and C_e are rates of k^{th} MT and capacity of the eavesdropper respectively. In case, if BS does not find any user greater than the

Table 2. SRS based selection algorithm

Initialization: $S = \emptyset$, BS transmits pilot signal and it knows the channel information of eavesdropper i.e. $\mathbf{H}_e$.
Step 1: Let $\mathbf{H} \in C^{K \times M}$ be the channel matrix of all active MTs and is defined as $\mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_K]$ where $\mathbf{h}_k \in C^{1 \times M}$ is the channel vector of the k^{th} MT and $k = 1, 2, \cdots, K$.
Step 2: Each MT measures its wireless channel $\mathbf{h}_k \in C^{1 \times M}$ and sends this information back to the base station.
Step 3: BS calculates the secrecy rate R_k^{sec} using Equations (4, 5, 8).
Step 4: BS orders all secrecy rates R_k^{sec} such that $\overline{R}_1^{sec} > \overline{R}_2^{sec} > \cdots, \overline{R}_K^{sec}$ where $\overline{R}_k^{sec}$ represents the ordered value of secrecy rate.
Step 5: Construct at the BS: $\overline{\mathbf{R}} = [\overline{R}_1^{sec}, \overline{R}_2^{sec}, \cdots, \overline{R}_K^{sec}]$.
Step 6: Select S MTs from $\overline{\mathbf{R}}$ such that $S = \{m_1, m_2, \cdots, m_S\}$ is the set of MTs for transmission.
Step 7: Calculate the precoding matrix for S selected MTs such that $\overline{\mathbf{W}} = [\overline{\mathbf{w}}_1, \overline{\mathbf{w}}_2, \cdots, \overline{\mathbf{w}}_S]$ where $\overline{\mathbf{w}}_k = \frac{\overline{\mathbf{h}}_k^H}{\|\overline{\mathbf{h}}_k\|}$.
Step 8: Transmit S MTs with the calculated secrecy rates.
Step 9: Terminate the algorithm.

secrecy rate, it does not transmit any user during that particular time slot. The complete SRS algorithm implemented at the BS is given in Table 2.

5 Numerical Results and Discussions

In this section we present some numerical results and prepare discussion on these results. First experiment is based on the total system capacity where we compare the sum-capacity lower bound results of massive MIMO with conjugate beamforming and zero forcing precoding as described in [19]. This sets the benchmarks for other results. Figures 3 and 4 show these results. The system is operating at -6.0 dB SINR and number of users are varied as $K = [16, 32, 64, 128]$. It is interesting to note that both results have different operational insight for the system. Figure 3 shows expected growth in system capacity along with base station antennas and number of users in the system. However, in Figure 4 with ZF precoding the system performance does not increase as that of with CB precoding and it shows a number of interesting crossing points as for as system operation is concerned. For example, for considerable large number of base station antennas, system performance still remains below 0 bits/sec/Hz which suggests that ZF precoding is not optimal under such conditions. It is also interesting to note that ZF with large number of users and base station antennas does not perform well compared to less number of users and base station antennas, for example, see the

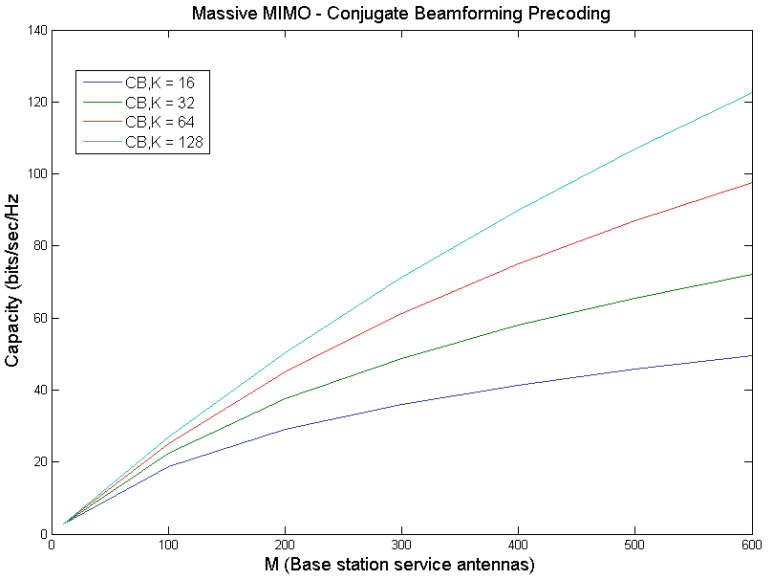

Fig. 3. Total capacity versus number of base station antennas for massive MIMO downlink with CB precoding.

curve with $K = 128$ users. One of the reasons for this poor performance could be that since ZF requires channel matrix inversion for nulling the interference, with large number of users and base station antennas this channel inversion may have some error and hence does not reduce the interference properly.

In figure 5, we show the sum rate per user with different user selection algorithms. The figure shows results of four different user selection algorithms. Black curve shows the sum rate when base station has perfect channel state information and we call this as perfect CSIT. This is the maximum data rate that base station can transmit theoretically since achieving perfect CSIT in practical systems is not feasible. The red curve shows Round Robin (RR) user selection algorithm when base station randomly selects M number of users and transmits them. In all the simulations we have $K = 100$ and $M = 50$. This result clearly shows inferior performance compared to other algorithms which shows that we need to apply some type of selection algorithm at the base station. However, one interesting feature of RR algorithm is that it is very simple to implement at the base station and does not require high computing resources. So in scenarios, where performance of the system does not matter very much, RR will be the algorithm of choice. Green curve in the figure shows Frobenius norm (FNS) user selection. In this algorithm as mentioned previously, base station calculates the Frobenius norm of all users and then selects M best users for transmission based on its channel norm. In blue curve, we show the result of eavesdropper capacity.

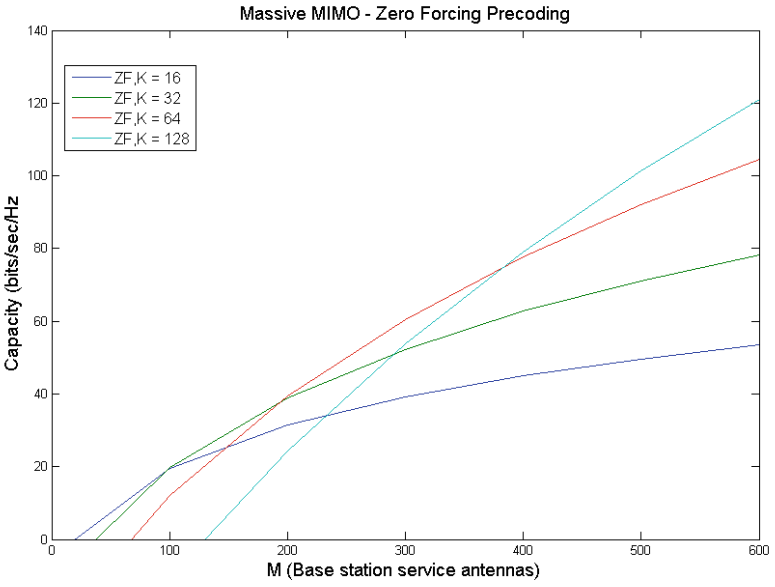

Fig. 4. Total capacity versus number of base station antennas for massive MIMO downlink with ZF precoding.

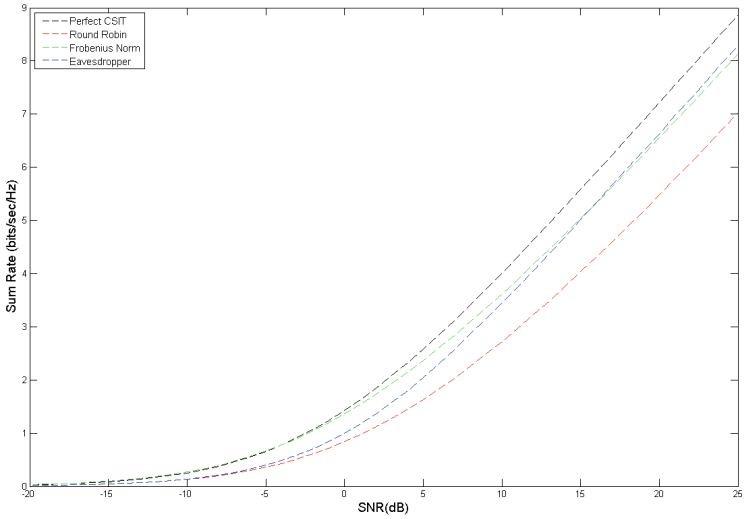

Fig. 5. Sum rate per user versus signal to noise ratio (SNR) with different user selection algorithms.

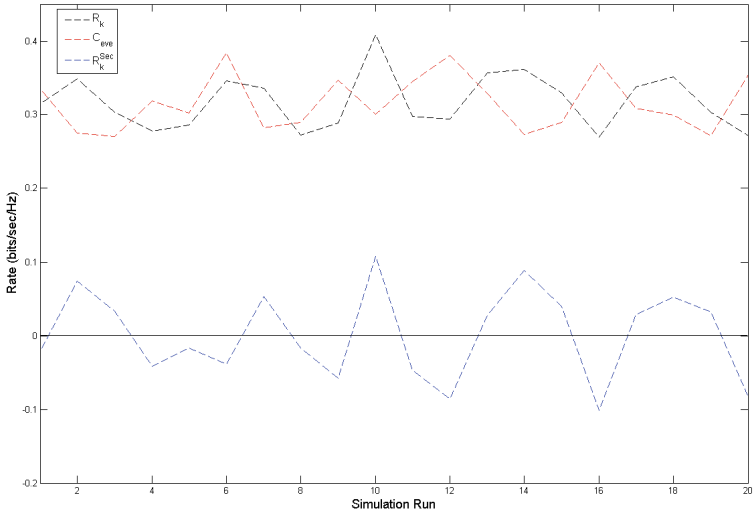

Fig. 6. Secrecy rate of a real user and eavesdropper comparison showing when user should be selected for transmission.

We assume that eavesdropper has perfect channel knowledge and it can achieve maximum capacity of single user equivalent. It is interesting to note that sum rates of FNS and eavesdropper cross each other at high SNR regime. In the proposed scheme if base station selects a user with its sum rate greater than eavesdropper rate then it is not possible for the eavesdropper to decode that users data.

Figure 6 shows an interesting implication that when a user must be selected for transmission securely. It shows the rate comparison of a single user with the rate of an eavesdropper and also shows the times when a real user is safe for selection without the ability of eavesdropper to decode its data. When the channel rate of a real user is higher than the data rate of eavesdropper, then it should be selected for transmission as shown in Equation (8). This result shows the evidence that it is not feasible for a user to be selected every time even though its channel may support a good data rate.

6 Conclusion

In this paper, we discussed the problem of user / device selection based on secrecy rate in massive MIMO downlink system. This is particular interesting for future 5G based systems where large number of users / devices are expected to share the available resources. Security, privacy and data integrity in such situations become even more important than in the systems today. Our results show that if a user / device is selected based on its secrecy rate, it has high probability of secure transmission. We have also shown the comparison of two precoding schemes for multi-user downlink scenarios. It is interesting to note that a user / device may not be suitable to transmit to every time if its data rate is less than the data rate of an eavesdropper. In future, we will extend these results with other layers and applications in the context of future wireless communication systems. Also we are interested in exploring the embedded security concept in future wireless networks.

References

1. Kapetanovic, D., Zheng, G., Rusek, F.: Physical Layer Security for Massive MIMO: An Overview on Passive Eavesdropping and Active Attacks (2015). http://arxiv.org/abs/org/pdf/1504.07154v1.pdf
2. Dean, T.R., Goldsmith, A.: Physical-Layer Cryptography through Massive MIMO (2013). http://arxiv.org/abs/org/abs/1310.1861
3. Mukherjee, A., Fakoorian, S.A.A., Huang, J., Swindlehurst, A.L.: Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey (2014). http://arxiv.org/pdf/1011.3754v3.pdf
4. Marzetta, T.L.: Noncooperative Cellular Wireless with Unlimited Number of BS Antennas. IEEE Transaction on Wireless Communications **9**(11), 3590–3600 (2010)
5. Rusek, F., Persson, D., Lau, B.K., Larsson, E.G., Marzetta, T.L., Edfors, O., Tufvesson, F.: Scaling Up MIMO: Opportunities and Challenges with Very Large Arrays. IEEE Signal Processing Magazine **30**(1), 40–46 (2013)

6. Larsson, E.G., Edfors, O., Tufvesson, F., Marzetta, T.L.: Massive MIMO for Next Generation Wireless Systems. IEEE Communication Magazine **52**(2), 186–195 (2014)
7. Zhu, J., Schober, R., Bhargava, V.K.: Secure Transmission in Multi-Cell Massive MIMO Systems. IEEE Transaction on Wireless Communications **13**(9), 4766–4781 (2014)
8. Biglieri, B., Calderbank, R., Constantinides, A., Goldsmith, A., Paulraj, A., Poor, H.V.: MIMO Wireless Communications. Cambridge University Press (2007)
9. Tu, Z., Blum, R.S.: Multiuser Diversity for a Dirty Paper Approach. IEEE Communication Letters **7**(8), 370–372 (2003)
10. Yoo, T., Goldsmith, A.: On the Optimality of Multi-antenna Broadcast Scheduling using Zero-Forcing Beamforming. IEEE Journal on Selected Areas in Communications **24**(3), 528–541 (2006)
11. Dimic, G., Sidiropoulos, N.D.: On Downlink Beamforming with Greedy User Selection: Performance Analysis and a Simple New Algorithm. IEEE Transactions on Signal Processing **53**(10), 3857–3868 (2005)
12. Oggier, F., Hassibi, B.: The Secrecy Capacity of the MIMO Wiretap Channel. IEEE Transactions on Information Theory **57**(8), 4961–4972 (2011)
13. Roy, S.: Two-Layer Linear Processing for Massive MIMO on the TitanMIMO Platform. Nutaq white paper on MIMO Platform (2015). http://nutaq.com/en/library/whitepaper-news/new-paper-two-layer-linear-processing-massive-mimo-titanmimo-platform
14. Paulraj, A., Nabar, R., Gore, D.: Introduction to Space-Time Wireless Communications. Cambridge University Press (2008)
15. Khan, M.A., Vesilo, R., Collings, I.B.: Efficient user selection algorithms for wireless broadcast channels. In: The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (2007)
16. Yanase, M., Ohtsuki, T.: User Selection Scheme with Secrecy Capacity in MIMO Downlink Systems. Procedia Social and Behavioral Sciences **2**, 161–170 (2010)
17. Boccardi, F., Heath Jr., R.W., Lozano, A., Marzetta, T.L., Popovski, P.: Five Disruptive Technology Directions for 5G. IEEE Communication Magazine, 74–80, February 2014
18. Wunder, G., Boche, H., Strohmer, T., Jung, P.: Sparse Signal Processing Concepts for Efficient 5G System Design. IEEE Access **3**, 195–208 (2015)
19. Marzetta, T.L.: Massive MIMO: An introduction. Bell Labs Technical Journal **20**, 11–22 (2015)
20. Hong, Y.-W.P., Pang-Chang, L., Kuo, C.-C.J.: Enhancing Physical Layer Secrecy in Multiantenna Wireless Systems: An Overview of Signal Processing Approaches. IEEE Signal Processing Magazine **30**(5), 29–40 (2013)