# PHYSICAL LAYER SECURITY ENHANCEMENT FOR MASSIVE MIMO SYSTEM: A REVIEW

**Sadaf Bukhari[1], M. R.Anjum[2]**
Department of Electronic Engineering, Islamia University of Bahawalpur, Pakistan
E-mail: [1]sadafbukhari02@gmail.com,[2]engr.muhammadrizwan@gmail.com

*ABSTRACT- Wireless security becomes a very important requirement as the advancement in technologies become growing day by day. As in fifth generation of mobile communication severe security requirements are needed for the transfer of information data like file transfer, business information and private emails etc. Massive MIMO plays an important role in next generation wireless communication, it is not only increases the throughput and reliability of system but also offer better physical layer security in wireless systems. Because of massive MIMO technique, it provides high antenna gain. In this paper Massive MIMO for the improvement of the security at physical layer has been discussed with different aspect of challenges and some recent techniques which may overcome these security issues.*

Keywords: Physical layer security, jamming, Massive MIMO, security.

## INTRODUCTION

Due to the advancement in multimedia technologies used in communication. Wireless networks channels are more vulnerable to attack. The security architectures provides security mechanism to prevent from attacks. OSI models architecture used seven layers such that physical layer, data link layer, network layer, transport layer, session layer, presentation layer and application layer as shown in Fig.1. There are different security mechanisms which are used according to the type of layer and protocols, In upper layers its essential requirement for data security [1].

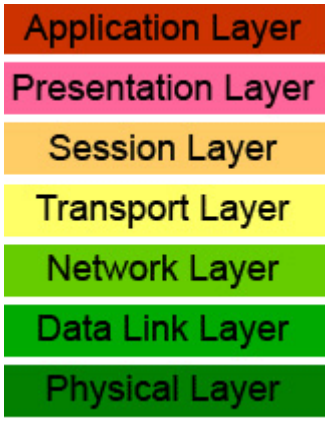


**Figure 1. Open Systems Interconnection (OSI) model**

In telecommunication the evaluation of generation, which moves from first to fourth and next to the fifth generation etc. Bandwidth also increases, as it is use to transmit the multimedia applications. In first generation of mobile networks, where there is only voice service used for communication purpose and in this generation there is no mechanism for security of voice calls available. In second generation mobile network uses the global system for mobile communication, onwards mobile services offer digital voice, data and international roaming. GSM provides end to end security by maintaining the confidentiality and authentication process. In the third generation the services are further increases likewise video conferencing, chatting, video on demand, TV mobile, digital images etc. 3G networks also uses CDMA, which inherently provides security. In the fourth generation mobile networks security techniques like substitution and confusion methods, end to end encryption and light weight cryptography used.

The encryption of data occurs at the upper layers (application layer, presentation layer) by using the cryptography. While at the physical layer there is also need for data security. For the security of physical links provided by the results of cryptography, signal processing and transmission of information, authentication, confidentiality and integrity are controlled at the upper layers of OSI model by different types of symmetric and asymmetric cryptosystem [2-3]. In wireless communication systems there is open channel between the transmitter and receiver and it has chances/ possibilities for transmitted information is eavesdrop or jammed by the eavesdropper or jammer respectively. Eavesdropping is the technique for getting the confidential information for analysis and storage. In wireless communication the eavesdroppers receives the transmitting radio waves and it is used for receiver to recover the data but not completely recovers. It is further divided into passive eavesdropping and active eavesdropping. Jamming attack is one of the type of denial of service attack. Jamming attacks affect propagating signals, protocols and wireless applications [4]. In communication jamming attacks are various types like signal total destruction, flipping of bits and insertion of fake signals. It is very difficult to detect the source of jamming attack and it is greatly depend on the type of network devices. In wireless communication physical layer security is also improved by using the MIMO technique, multiuser MIMO and further by the massive MIMO technique. Massive MIMO technique is an emerging solution for increasing the capacity, throughput and reliability of $5^{th}$ generation of mobile communication technology. On the other hand it also offer an advancement in communication security [5-6].

## MASSIVE MIMO

Massive MIMO carries large scale antenna system and used in fifth generation of wireless communication. In this technique large number of antennas is used at the base station

to fulfill the requirements of large number of users at a time. In fourth generation of wireless communication LTE (long term evaluation) allows only multiple antenna ports at the base station; in this way. Massive MIMO increases the throughput, spectral efficiency, reliability and capacity of the system. It also immune to fading interference and intentional jamming attacks.

It uses the time division duplexing (TDD) operation or somehow uses the frequency division duplexing operation. FDD technique carries the channel estimation process depends on the number of antennas used at the base station while TDD uses large number of antennas at the base station because the channel estimation process does not depend on the number of antennas [7-8]. Massive MIMO also enhanced the physical layer security in wireless communication; by using large number of antennas at the base station, it increases the array gain towards the intended users and the eavesdropper received the small power signal.

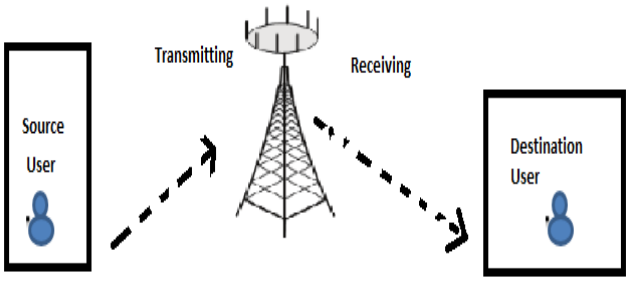


**Figure 2. Massive MIMO Architecture**

Iterative algorithm carries the transmitted signal vector and power of the user by the game theory in the presence of eavesdropper and jammer it require to maintain signal to interference plus noise ratio (SINR) [10 -11].

## CONCLUSION

In this paper, the importance of security in wireless communication has been discussed. As the technology in mobile communication is growing up the security aspects is also going to become more critical at the physical layer, the attackers are going to become more advance in hacking and stealing the data or information. Massive MIMO improves some security issues but also it has challenges in which the main is pilot contamination: less accuracy in channel state information of main channel and wiretap channel at the legitimate transmitter. Finally, recent techniques to overcome security challenges discussed but from future aspect more research are required to solve these security challenges in the next generation of telecommunication evolutions system.

## REFERENCES

1. Zhou, Xiangyun, Lingyang Song, and Yan Zhang, eds. “Physical Layer Security in Wireless Communications”. Crc Press, 2013.
2. Mukherjee, Amitav, et al. "Principles of physical layer security in multiuser wireless networks: A survey." IEEE Communications Surveys & Tutorials 16.3 (2014): 1550-1573.
3. Stallings, William. “Cryptography and network security: principles and practices”. Pearson Education India, 2006.
4. “An overview on passive eavesdropping and active attacks." IEEE Communications Magazine 53.6 (2015): 21-27.
5. Ngo, Hien Quoc. Massive MIMO: “Fundamentals and system designs”. Vol. 1642. Linköping University Electronic Press, 2015.
6. Zhang, Xi, et al. "Artificial-noise-aided secure multi-antenna transmission with limited feedback." IEEE Transactions on Wireless Communications 14.5 (2015): 2742-2754.
7. Zou, Yulong, et al. "A Survey on Wireless Security: Technical Challenges”, Recent Advances, and Future Trends." (2015).
8. Zhu, Jun, Robert Schober, and Vijay K. Bhargava. "Physical layer security for massive MIMO systems impaired by phase noise." arXiv preprint arXiv:1603.01869 (2016).
9. Deng, Yansha, et al. "Safeguarding massive MIMO aided hetnets using physical layer security." Wireless Communications & Signal Processing (WCSP), 2015 International Conference on. IEEE, 2015.
10. Rawat, Danda B., Kishan Neupane, and Min Song. "A novel algorithm for secrecy rate analysis in massive MIMO system with target SINR requirements." Computer Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference on. IEEE, 2016.
11. Chen, Xiaoming, Jian Chen, and Tao Liu. "Secure transmission in wireless powered massive MIMO relaying systems: Performance analysis and optimization." (2015).