International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 07, July 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Software Defined Internet of Things (IoT) in 5G Millimeter Wave (mmWave) Communication System

S. K. Agrawal[1], Dr. Kapil Sharma[2]

[1]*Samsung Research Institute Noida, (India)*

[2]*Computer Engineering Department, Delhi Technological University, (India)*

ABSTRACT

This research paper discusses software defined secure Internet of Things (IoT) data transmission in 5G millimeter wave (mmWave) communication system. The proposed software defined system dynamically interleaves the data before transmission in in 5G mmWave communication system. Software defined secure 5G mmWave communication system randomly transmits the dynamically interleaved data and the interleaved parameters to the desired IoT device. The IoT receiver performs dynamic de-interleaving of the received data using the received interleaved parameters.

Keywords - Millimeter Wave (mmWave); software defined (SD); Software Defined Random Skip Count (SDRSC)

I. INTRODUCTION

5G mmWave Communication is an emerging technique that helps to increase data capacity across the globe by having mmWave communication link. 5G mmWave communication will facilitate various advance IoT applications like IoT, Virtual Reality (VR) , Augmented Reality (AR) and etc. Further IoT devices are also involved in various transactions, data exchange, payments and so on. Further, 5G mmWave IoT Communication enabled devices can be used to view real time information and to purchase items. IoT devices are equipped with transceivers are capable of sending an encrypted data to the other IoT devices [1-5].

5G mmWave IoT communication system requires security for data. The 5G IoT data can be captured and decoded which will lead to loss of sensitive data. The data transmitted using 5G mmWave IoT communication system may be demolished using a jammer. The 5G mmWave IoT communication data can be prone to data modification attacks if not transmitted securely. 5G mmWave IoT communication can suffer man-in-the-middle attack and important transaction may take the incorrect results. Various kind of attacks can critically affect the 5G mmWave IoT communication. Interleaving has been used for avoiding the noise and it permits arrangement of data in specific row and column formats. In 5G mmWave IoT communication; there is a demand and need for a secure method for ensuring data security in 5G mmWave IoT communication system [6-9].

5G Millimeter Wave (mmWave) communication system growth also inviting attention of IoT along with security. 5G IoT will provide pervasiveness and ubiquity with mmWave communication system. IoT for a common user will increase interaction with user common devices and will interact in virtual or augmented mode having IoT connectivity. The method proposed here is reliable and highly precise secured to prevent IoT data loss and IoT data leakage [10-15].

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

This paper is organized as follows: Section II describe the dynamic interleaving in 5G mmWave IoT communication system. Sections III describe the dynamic interleaving steps in 5G mmWave IoT communication system. Further section IV describe the system architecture for dynamically data interleaving in 5G mmWave IoT communication system. This research object is to enable a secured 5G mmWave IoT communication system among IoT devices. It improves security in 5G mmWave IoT communication system by implementing dynamic interleaving using randomization.

II. DYNAMIC INTERLEAVING IN 5G MMWAVE IOT COMMUNICATION SYSTEM

Accordingly the research provides a system for facilitating a secure 5G mmWave IoT communication between a first IoT device and a second IoT device. In this system, the first IoT device transmits secure interleaved data dynamically to the second IoT device, using randomization technique. Further, the first device transmits the dynamically interleaved data to the second device. The first device also transmits dynamically interleaved parameters to the second device. Further, upon receiving the dynamically interleaved data and parameters from first device, the second device de-interleaves received data.

The research system enables secured IoT data communication by having randomizer based dynamic interleaving tool. In this system, data to be transmitted using 5G mmWave IoT communication system is interleaved in a specific format and interleaved data is sent to the other IoT device. The IoT transmitter also sends dynamic interleaving parameters which are used for interleaving the data, to the destination IoT device through secured 5G channel or by having a certificate authority (CA). The dynamically interleaved IoT data and dynamic interleaving parameters can be sent to the destination IoT device using same 5G communication channel. The dynamically interleaved IoT data and dynamic interleaving parameters can be sent to the destination IoT device through different channels and by using separate 5G communication channels for IoT data transmission increases security in the data transmission.

5G mmWave IoT communication system dynamic interleaving can be performed in 2-dimensional matrix. In a 2-dimensional model, the IoT data to be transmitted using 5G can be arranged in a 2 dimensional (2D) matrix by using SDR based architecture. 2D matrix has form of Rows and Columns. In this security method, the 5G mmWave IoT communication system has to calculate parameters such as quantity of rows (m), quantity of columns (n), data filling / releasing format. System further has capability for Random Row (Dm) / column Selection for filling the matrix and Random Column (Dn) / Row Selection for releasing the IoT data from matrix and so on for arranging the IoT data in matrix in the random fashion using SDR.

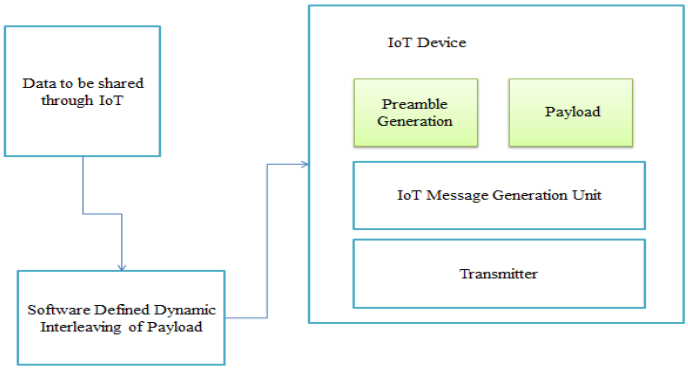

Figure 1: Dynamically Data Interleaving Before Transmission for 5G mmWave IoT Communication System

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

FIG. 1 illustrates a block diagram which shows various components of a IoT device. The IoT device comprises transmitter antenna; software defined dynamic interleaving of payload, IoT message generation unit, preamble generation and etc. The IoT transmitter antenna can be used to send and receive IoT and IoT message generation unit facilitates transfer of messages from the IoT device. The IoT device can send a new message and/or view a received message using the secure module. The IoT deice facilitates 5G mmWave IoT communication system between IoT devices.The proposed system enables secured data communication by incorporating a randomization based dynamic interleaving scheme. Using the dynamic interleaving scheme, the 5G mmWave IoT communication system devices interleaves the IoT message to be transmitted, in a specific format and transmit to the destination IoT device. The 5G mmWave IoT communication system device improves IoT data security in transmission.

III. DYNAMIC INTERLEAVING STEPS IN 5G MMWAVE IOT COMMUNICATION SYSTEM

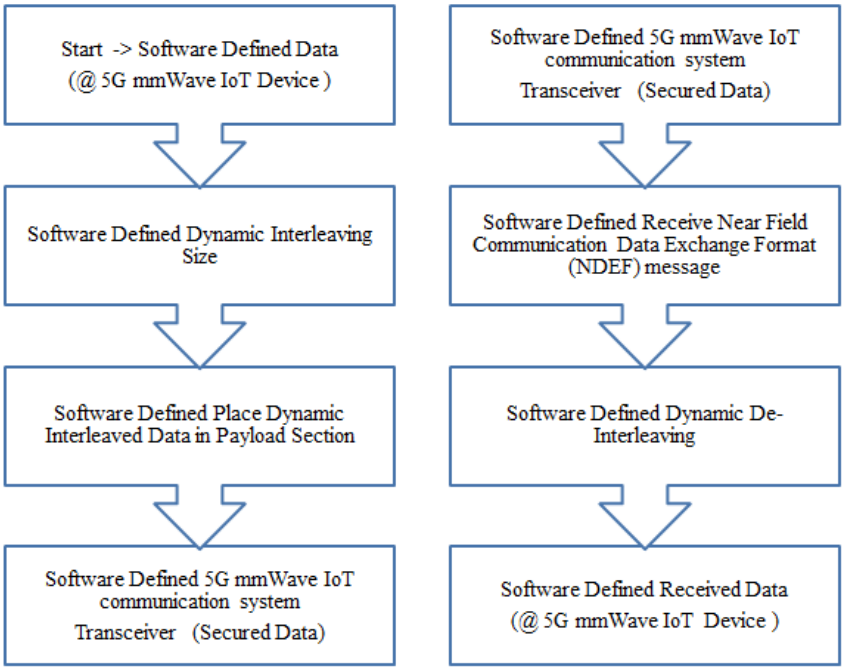

Figure 2: Dynamically Data Interleaving Between 5G mmWave IoT Communication Devices

FIG. 2 illustrates a various stages and steps of software defined secure Internet of Things (IoT) in 5G mmWave communication system. The IoT device comprises preamble generation element, dynamic interleaved payload generation element, IoT message generation element , transceiver, IoT message detection element , preamble detection element and dynamic de-interleaved payload generation element. The preamble generation element 301 generates preamble of the IOT message to be transmitted. The preamble part of the message can be used to obtain synchronization between the transmitted and received messages. An example of the preamble of a message can be header of the message. Further, length of the preamble affects packet overhead of the message and can accordingly affect transmission time of the message. The IoT dynamic interleaved payload generation element generates dynamically interleaved payload IoT data. The dynamic interleaved payload generation element implements a dynamic interleaving algorithm in order to ensure high level security in the IoT data

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

transfer. The IoT dynamic interleaved payload generation element interleaves the data to be transmitted into a specific format using randomization technique. IoT dynamic interleaved payload generation element can safeguard the data at the time of any attack or communication failure or hacking.

IoT message generation element generates the IoT message to be transmitted to a destination IoT device. The IoT message can be generated by arranging in order the preamble and the dynamically interleaved payload in a particular sequence as specified by the 5G communication protocol used for data transmission between the IoT devices. The IoT transmitter transmits the IoT message generated by the IOT message generation element and also transmits interleaved parameters to the destination IOT device. IoT transmitter can transmit the IOT message and the interleaved parameters using same 5G communication channel at different time. IoT transmitter can transmit the interleaved parameters through different secured 5G channels. IoT data transmission can also take place through an authorized certification authority (CA). IoT receiver element receives the dynamically interleaved data and/or the interleaved parameters transmitted by the IoT transmitter. The IoT preamble detection element processes the received interleaved information and detect the preamble in the received IOT message.

The IOT message is passed onto the dynamic de-interleaved payload generation element. The dynamic de-interleaved payload generation element performs de-interleaving of the received IOT message to identify the payload data. The dynamic de-interleaved payload generation element can use the interleaved parameters received from the IoT transmitter of the sending IoT device. Using the interleaved parameters , the dynamic de-interleaved payload generation element, the dynamic de-interleaved payload generation element perform de-interleaving of the received IOT message. IOT message detection element processes the received information and constructs the original IOT message.

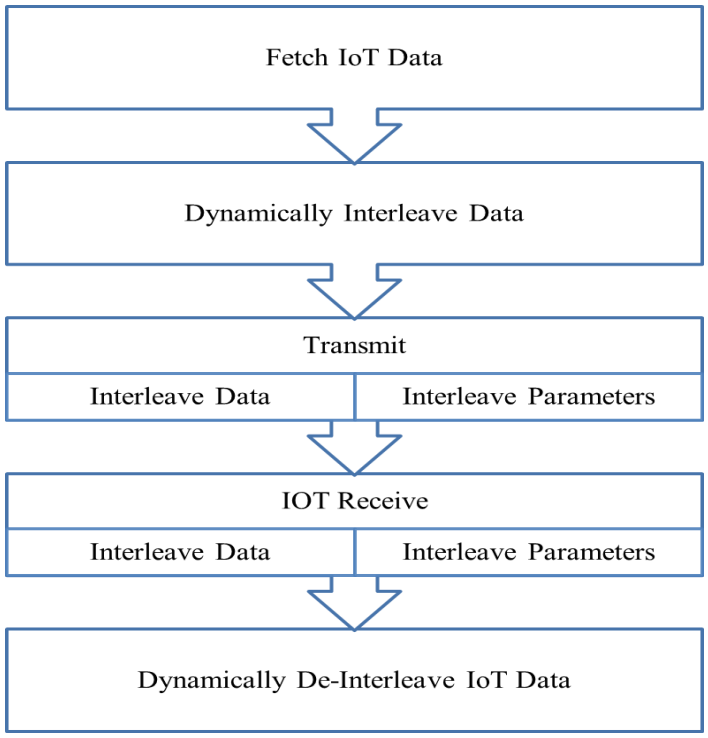

Figure 3: Dynamically Data Interleaving Steps

FIG. 3 illustrates research flow diagram which depicts various steps involved in the process of IoT dynamic interleaving and dynamic de-interleaving of data. IoT data is fetched by the dynamically interleaved payload

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

generation element and dynamically interleaved payload generation element performs dynamic interleaving of the data. IoT dynamic interleaving of data is performed by using randomization of data in interleaving fashion. The dynamic interleaved data is transmitted to the destination IoT device using a transmitter in the sender IoT device.

IoT data can be dynamically interleaved in the form of a 2-dimensional matrix. Software defined secure IoT system can use dedicated randomizers for the purpose of 2D interleaving and dynamic interleaving can also be done after generating the message or packet. The proposed dynamic interleaving mechanism does not require addition of any extra additional bits for security of the IoT data. This helps to maintain same IoT data size even if the IoT data is dynamically interleaved. Software defined secure IoT system parameters are not always shared with other IoT devices. If both IoT devices are paired or agreed to share the data based on certain parameters , the certain parameters can be used for the data sharing and no need to send the parameters every time with the data. In case of any attack or loss of data, the parameters are shared with the IoT device.

The interleaved data is received by the IoT receiver element in the receiver IoT device. The SDR receiver shall be aware that the dynamic interleaving is done after packet generation or before the packet generation. Further, the IoT receiver checks if the received data is new or if the data transmission is affected by hacking or data loss or any such issues. If the received data is new or if the data transmission is affected by hacking or data loss or any such issues, the receiver receives new IoT dynamic interleaved parameters from the data transmitter. If not, the receiver use (706) already received dynamic interleaved parameters to dynamically de-interleave the received de-interleaved data. In an , the proposed mechanism does not require the IOT receiver to receive dynamic interleaved parameters each time the data is transmitted. The IoT dynamic de-interleaved payload generation element present in the receiver IoT device performs dynamic de-interleaving of the received data using the dynamic interleaving parameters received from the transmitter IoT device.

II. SYSTEM ARCHITECTURE FOR DYNAMICALLY DATA INTERLEAVING IN 5G MMWAVE IOT COMMUNICATION SYSTEM

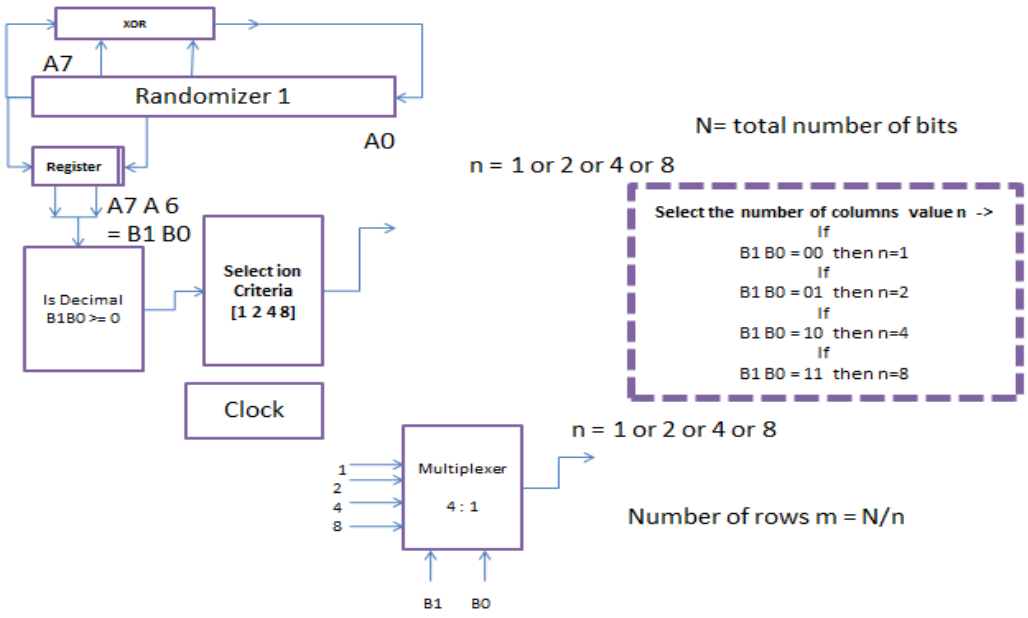

Figure 4: System Architecture for Dynamically Data Interleaving

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Figure 4 illustrates software defined secure IoT system architecture for measuring number of rows and number of columns using randomizers. For a 2-dimensional matrix, if number of rows (m) is calculated using randomizer, then the number of columns (n) is calculated using a suitable equation or else if the number of columns (n) is calculated using randomizers, then the number of rows (m) is calculated using a suitable equation. In the proposed software defined secure IoT system architecture for calculating number of rows or columns, the randomizer is initiated by inputting a bit sequence. A random IoT clock shift is performed to the inputted IoT bit sequence and two bits from pre-defined location in the bit sequence are fetched for IoT. Fetched bits are compared with a IoT look up table and table can comprise number of rows (m) to be selected corresponding to the fetched bit sequences for IoT. Based on the value in table the system selects/decides the number of rows (m) for the 2D matrix. Software defined secure IoT system architecture for calculating data filling/releasing format for a 2D matrix, the randomizer is initialized by inputting a bit sequence of suitable length to the randomizer. The selected IoT data filling/releasing format is used for data filling/releasing to and from the 2D matrix. The bits can be picked from any place in the sequence, as set by the software defined secure IoT system and bits can be tapped from any set location.

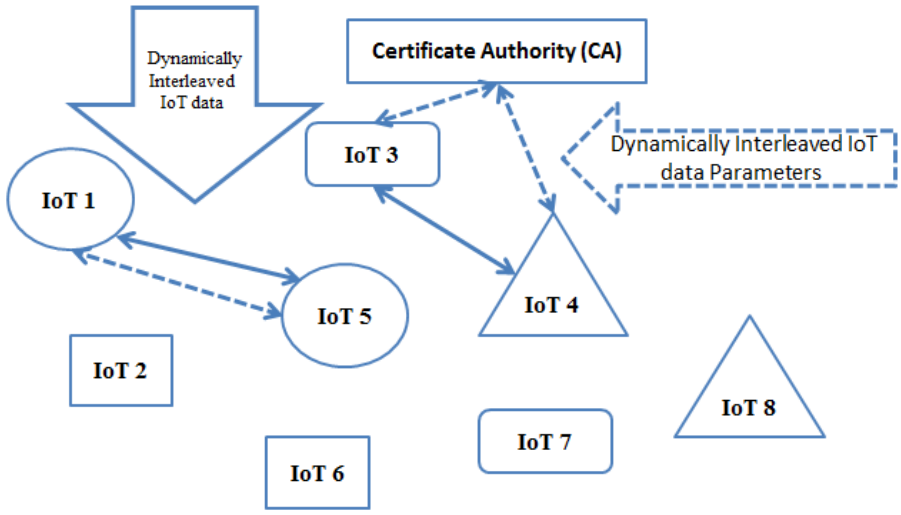

Figure 5: System Architecture for Sharing Dynamically Data Interleaving Data and Parameters

Figure 5 illustrates SDR system architecture for sharing dynamically interleaved IoT data and parameters between sender IoT and receiver IoT. The data to be transmitted from the IoT device to the destination IoT device is dynamically interleaved in the IoT devices like as shown IoT 1 to IoT 8. The dynamically interleaved data and the dynamic interleaving parameters are shared with the destination IoT device in one to one manner or through central server or CA. The dynamic interleaved IoT data and the dynamic interleaved IoT parameters can be shared through different 5G channels for better security. The dynamic interleaved IoT data and the dynamic interleaved IoT parameters can be shared through same channels having different time slots for better security. The dynamic interleaved IoT parameters corresponding to a dynamically interleaved data stream is shared only once between the IoT devices. The IoT parameters can be retransmitted for a IoT data only if any hacking takes place. The IoT parameters can be transmitted before the dynamically interleaved IoT data so that the receiver can perform real time de-interleaving of the IoT data. The channel used for sharing dynamically interleaved IoT parameters shall be secured channel and authorized certificate authority (CA) in 5G software defined secure IoT system.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

V. CONCLUSION

This paper discussed about facilitating a secure Internet of Things (IoT) data transmission in 5G millimeter wave (mmWave) communication system. In this paper, the first IoT device dynamically interleave the information and transmits to the second IoT device by having randomized interleaving . The IoT device transmits the dynamically interleaved data to the other device and also transmits dynamically interleaved parameters to the second IoT device. After receiving the dynamically interleaved data and parameters from first IoT device, the second device de-interleaves received data. Accordingly the paper discusses a secure Internet of Things (IoT) data transmission in 5G millimeter wave (mmWave) communication system. In Future work; to improve security level in IoT data transmission, the system can use software defined random skip count (SDRSC) values to generate new random skip count value based parameters to dynamically interleave the IoT data .

VI. ACKNOWLEDGMENT

This paper is specifically meant for educational purpose for completing Ph.D. degree with Delhi Technological University (DTU), Delhi India. This paper is prepared for submission to under Ph.D. progress. The authors are very much thankful to Samsung Research Institute Noida, India and Delhi Technological University (DTU) earlier recognized as Delhi-College of Engineering (DCE), New Delhi, India.

REFERENCES

[1] Zhouye Pi et al., “An Introduction to Millimeter- Wave Mobile Broadband Systems, ” IEEE Communications Magazine, vol.49, no.6, pp.101- 107, Jun. 2011.

[2] Andrews J.G. et al., “What Will 5G Be?, ” IEEE JSAC Special Issue On 5G Wireless Communication Systems, May 2014.

[3] Theodore S. Rappaport et al., “Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!, ” IEEE Access, vol.1, pp.335-349, May 2013.

[4] Wonil Roh et al., “Millimeter-wave Beamforming as an Enabling Technology for 5G Cellular Communications: Theoretical Feasibility and Prototype Results, ” IEEE Communications Magazine, vol. 52, no. 2, pp. 106-113, Feb. 2014.

[5] Samsung, “5G Vision, ” DMC R&D Center, Samsung Electronics Co., Ltd., Feb. 2015.

[6] Wei L. et. al., “Key Elements to Enable Millimeter Wave Communications for 5G Wireless Systems, ” IEEE Wireless Communications, vol.1, pp.136-143, Dec. 2014.

[7] Palattella, Maria Rita, et al. "Internet of things in the 5G era: Enablers, architecture, and business models." IEEE Journal on Selected Areas in Communications 34.3 (2016): 510-527.

[8] Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed internet of things." Computer Networks 57.10 (2013): 2266-2279.

[9] Babar, Sachin, et al. "Proposed embedded security framework for internet of things (iot)." Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on. IEEE, 2011.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[10] S. K. Agrawal and K. Sharma, "Software Defined Millimeter Wave 5th Generation Communications System", Application and Theory of Computer Technology, [S.l.], v. 2, n. 1, p. 46-56, Jan. 2017. ISSN 2514-1694

[11] S. K. Agrawal and P. Garg, "Calculation of Channel Capacity Considering the Effect of Different Seasons for Higher Altitude Platform System", Wireless Personal Communications, Springer, Wireless Personal Communications: vol. pp-719-729, Issue 4 2010.

[12] S. K. Agrawal and K. Sharma, "5G Millimeter Wave (mmWave) Communication System with Software Defined Radio (SDR)", International Conference on Recent Trends in Engineering & Science (ICRTES-16), 29th-30th September 2016, ISBN : 978-93-86171-06-1

[13] S. K. Agrawal and K. Sharma, "5G Millimeter Wave (mmWave) Communication System with Software Defined Radio (SDR)", International Journal for Innovative Research in Science & Technology, Volume 2, Issue 9, September 2016

[14] J. Mitola. III, "Technical Challenges in the Globalization of Software Radio,'' IEEE Commun. Mag., Feb. 1999, pp. 84–89.

[15] Yang L-L, Hanzo L. Software-defined-radio-assisted adaptive broadband frequency hopping multicarrier DSCDMA. IEEE Commun Mag 2002;40(3):174–83.