Asian Journal of Scientific Research, 2015
ISSN 1992-1454 / DOI: 10.3923/ajsr.2015.

Error Control Code Based Resistance against Primary User Emulation Attack in Cognitive Radio

J. Avila and K. Thenmozhi
Department of ECE, School of EEE, SASTRA University, Thanjavur, 613401, Tamil Nadu, India

Corresponding Author: J. Avila, Department of ECE, School of EEE, SASTRA University, Thanjavur, 613401, Tamil Nadu, India

ABSTRACT

Cognitive Radio Networks (CRN), one of the emerging technologies in the wireless communication domain, is primarily used for spectrum sensing and proper allocation of the unused licensed bands to the secondary users without causing any interference to the primary user in a dynamic manner. However, security to the physical layer becomes a major problem here. This study gives a reliable solution to avoid the Physical User Emulation Attack (PUEA) by employing a Pseudo noise sequence (PN) based novel encryption technique. This study brings out the MATLAB simulated BER curves before and after using the proposed algorithm interpreting the error performance. The results prove that the proposed algorithm gives a reliable real time performance.

Key words: Cognitive radio, PUEA, PN sequence, turbo codes, convolutional code, concatenated code

INTRODUCTION

Among the spectral bandwidths available, not all the spectral frequencies are used effectively. The white spaces (unused licensed spectrum bands) produces dearth of frequencies required for wireless communication. Hence, to utilize the spectrum effectively, Federal Communications Commission (FCC) brought forth a new technology, Cognitive Radio Network (CRN) (Haykin, 2005; Mitola, 2000). The CRN senses the available band of licensed frequencies that are unused by the primary user. In order to avail those frequencies, they are allotted to the requesting secondary user in such a way that the primary user does not face any interference. But the primary disadvantage is security. Here, the secondary users are forced to vacate the spectrum by third party members. This Denial-Of-Service (DOS), applicable for both primary user and secondary user, is due to the emulation of the primary user signals by the (third party members) known as Malicious Users (Chen *et al*., 2008). Physical layer is more prone to attacks by malicious users (Jin *et al*., 2009). The physical layer security, sought after to improve the efficacy of Cognitive Radio Networks (CRN), provides considerable robustness to the processed data even with the presence of malicious users.

The convolutional encoder is as shown in Fig. 1. Convolutional codes are similar to block codes. In block codes the message bits are sent. But, in convolution code only the parity bits are sent. In convolutional codes the messages are sent bit by bit. The constraint length is decided by the number of stages of the shift register. The output from the shift register is XORed to get the output which decides the rate of the convolutional code (Viraktamath and Attimarad, 2010; Nyirongo *et al*., 2006). At the receiver side viterbi decoder is used to extract the transmitted sequence.

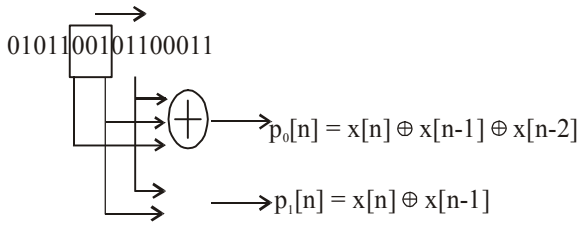

Fig. 1: Convolutional code with constraint length 3 and two parity bits per message bit

Turbo codes, serial concatenation of two convolution codes, introduced in 1993 are constructed by using two or more component codes on different interleaved iterations of the same information sequence. The interleaver can either serially connected to the convolutional codes or it may be parallel concatenation (Hoshyar *et al*., 2000; Avila *et al*., 2012).

Binary Phase Shift Keying (BPSK) can also be referred to Phase-Reversal-Keying (PRK). In BPSK, the signal to be modulated has constant amplitude. Depending on the level the data represents, the phase change occurs by 180°. Since it involves dealing with the highest level of noises and distortions, it is considered as the most robust modulation scheme among other PSKs. The main drawback is that this can be capable of modulating to the maximum of only one bit per symbol, thereby making it inefficient for larger data bits (Kumar and Sharma, 2007).

Quadrature Phase Shift Keying (QPSK) modulation technique is also referred to quadri-phase PSK. In QPSK, two bits are represented by a symbol and it is often misconstrued to have twice the data rate compared to BPSK without altering the signal bandwidth. The disadvantage is that the transmitters and receivers used in this modulation are more complicated and at the receiving end, phase ambiguity problems occur (Sklar and Ray, 2001).

In Quadrature Amplitude Modulation (QAM), two carrier signals with 90° phase change are modulated and the modulated signal consists of amplitude and phase variations. Here, one signal (Q) is represented by a sine wave and the other signal (I) by a cosine wave. This modulation can be viewed as a fusion of amplitude and phase modulation. Since it is a combination of AM and PM, it doubles the effective bandwidth.

This work focuses on mitigating the primary user emulation attack by means of a helper node sending authenticated information to the cognitive user about the availability of the primary user. The authentication tag is generated and embedded in the forward error control codes. The performance of the system is validated by means of bit error rate versus signal to noise ratio curve.

MATERIALS AND METHODS

Pseudorandom patterns are sufficiently random in nature to replace truly random sequences. The pseudorandom sequence is a deterministic, periodic signal and can be used as a key for encoding in the transmitter and decoding in the receiver. Even though the sequence is deterministic, it appears to take on the properties of sampled white noise, thus earning the right to be called as a pseudorandom sequence. Linear Feedback Shift Registers (LFSRs) are used in a widespread manner for generating test patterns for combinational circuits because they are easy to implement.

Not all binary ones and zeros are called as PN sequence. A PN sequence is called so if it satisfies the properties named:

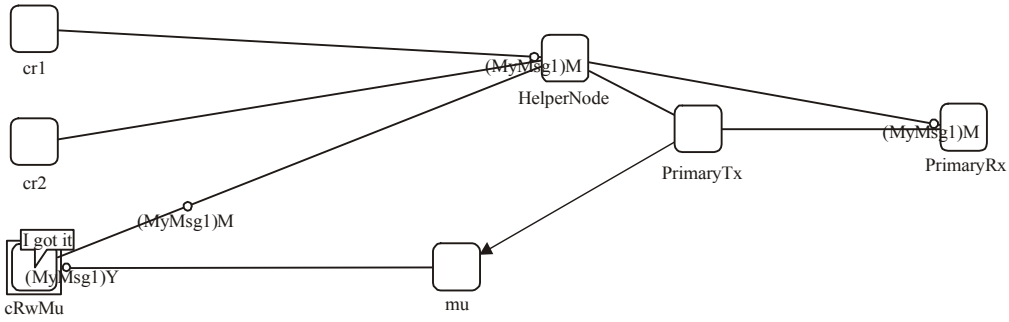

Fig. 2: Proposed method

- Balance property
- Run property
- Correlation property

The following sequence satisfies all the above mentioned properties and is said to be a perfect PN sequence:

0 0 0 1 0 0 1 1 0 1 0 1 1 1 1

Satisfying the above quoted properties, a PN sequence is generated and is embedded within the convolution encoded and turbo encoded message signal. PN sequence is used as the authentication tags. PN sequences are generated either in random or by some manual evaluation process. The randomly generated sequences are preferred over the other. These tags can be embedded in the error-correcting codes (Holmes and Chen, 1977; Ward, 1965).

Helper nodes: A helper node, a physical structure, is assumed to be in a very nearer range to the primary user. The helper node senses the availability of the primary user. If the primary user is absent the helper node sends the information to the cognitive user along with the authentication tag. The tag is embedded in the parity bits of the error control code. The number of bits are embedded in such a way that there is not much difference between in the Bit Error Rate (BER) between the system before embedding and embedding the tag (Salem *et al*., 2014).

Figure 2 shows the proposed method. In the wireless environment one primary user and its intended primary receivers are considered. Along with them three cognitive users, one helper node and one malicious user are also present. The helper node is closer to the primary user. It checks the availability of the primary user. If a spectrum hole is available then it sends that information to the cognitive user along with the authentication tag. The malicious user may also send false information about the presence of the primary user. But that information is simply discarded by the cognitive user. It relies only on the information with the authentication tag.

RESULTS AND DISCUSSION

Kim (2011) proposed the authentication protocol based on the location. The location information is the vital factor to maintain security and privacy. Nomura *et al*. (2011) proposed location based

authentication protocol. They named the protocol as EAP-CRP. Taheri *et al*. (2012) used two key encryption algorithm to prevent the system from attackers. Liu *et al*. (2010) used link signatures to authenticate the primary user. Hash function is used to generate the link signature. Chen *et al*. (2008) utilized the received signal strength to detect the location of the primary user. From the knowledge of the primary user the malicious user could be fount out. Pu and Wyglinski (2014) used database scheme to find out the malicious user. Trust based authentication scheme was proposed by Parvin *et al*. (2010). The behavior of the secondary user is analyzed and based on the trust value decisions are made. In the study of Kumar *et al*. (2012) embedding of tag is done in the precoder bits of duo-binary scheme. Alahmadi *et al*. (2014) used Advanced Encryption Standard (AES) algorithm as the authentication tag. They are embedded in the synchronization bits of the primary user's data frame.

In this study embedding of the tag is done in the parity bits of turbo code and since the coding gain of the concatenated code is better than the single code embedding is done in the concatenated code. Here convolutional code is concatenated with turbo code. Simulation results are concluded from the bit error rate versus Eb/N0 curve. Figure 3 gives the comparison between the PN sequence embedded in the parity bits of turbo code and convolutional code. From the figure it is evident that there in an improvement in BER as well as Eb/No in the case of turbo code.

Figure 4 shows the comparison between convolutional code and convolutional code concatenated with turbo code. From the Fig. 4 it is clear that concatenated code offers good BER than individual code. This is because the coding gain of the concatenated code is higher than the single one. Here, PN sequence is embedded in the parity bit of the concatenated code.

Figure 5a shows the comparison between BPSK, QPSK and QAM modulation schemes. Here, the tag which is nothing but the pn sequence is embedded in the parity bits of the turbo code. Figure 5b shows the comparison between BPSK, QPSK and QAM modulation schemes. Here the tag which is nothing but the pn sequence, is embedded in the parity bits of the turbo code concatenated with convolutional code. Simulation result proves that BPSK is better when compared

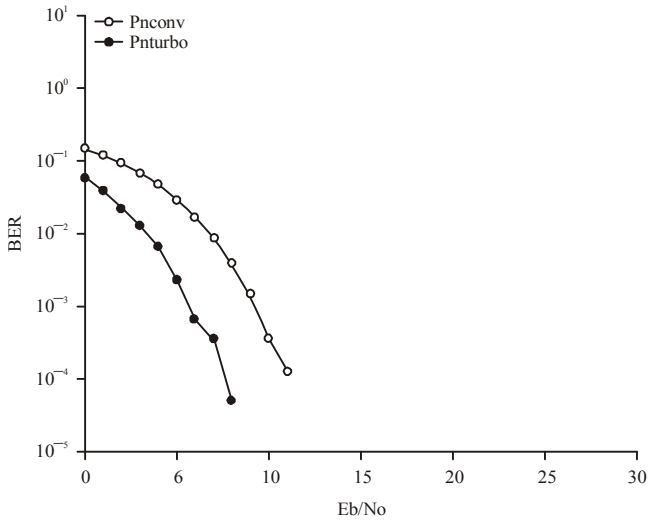

Fig. 3: Comparison between turbo code and convolutional code

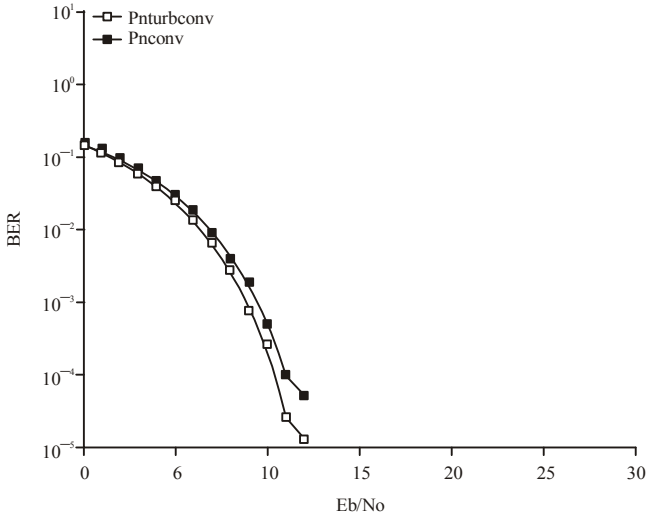

Fig. 4: Concatenated scheme

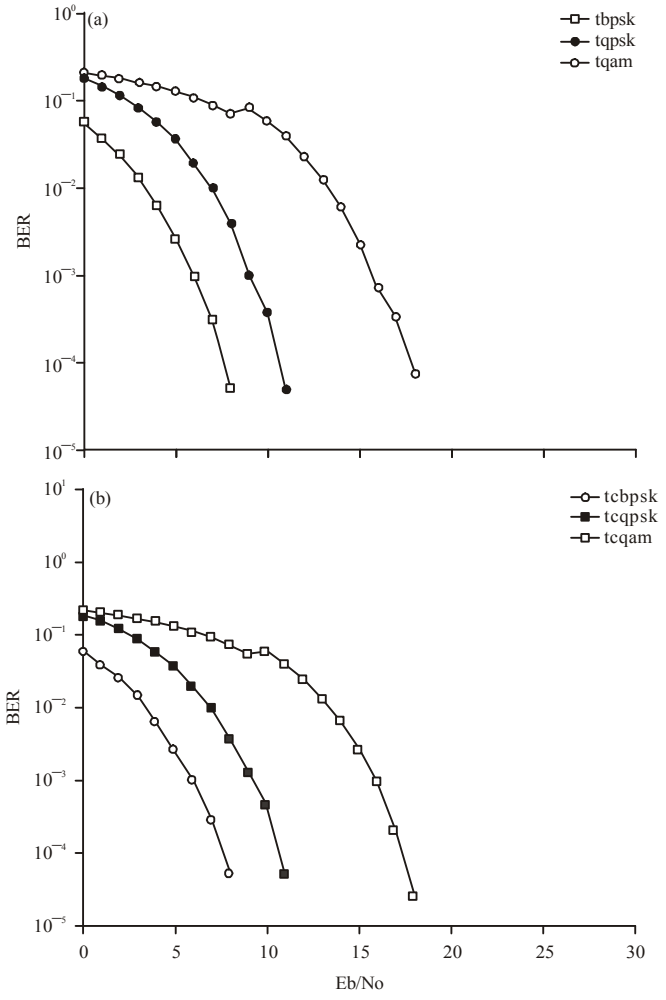

Fig. 5(a-b): PN sequence embedded in turbo code, concatenated scheme (a) PN turbo and (b) PN turbo covolution

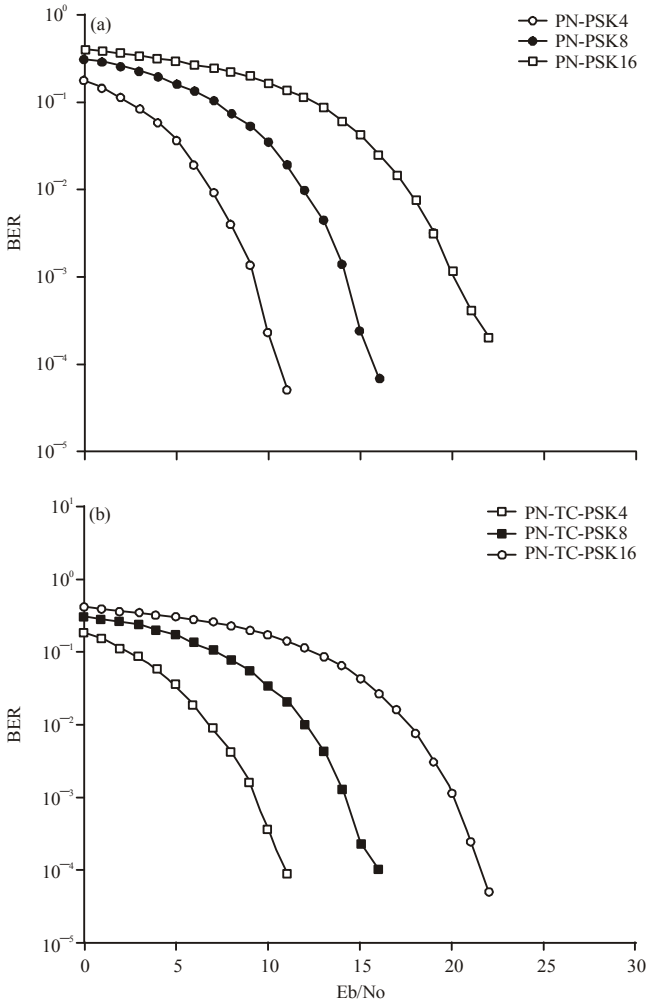

Fig. 6(a-b): PN sequence embedded in M-ary PSK, concatenated output, (a) PN turbo PSK and (b) turbo covolution

with other modulation schemes. It is less error prone when compared to QAM because of lesser number of signal points which in turn increases the distance. Higher is the distance better is the immunity to noise.

Figure 6a shows the comparison between M-ary PSK modulation schemes. Here the tag which is nothing but the pn sequence is embedded in the parity bits of the turbo code. Figure 6b shows the comparison between M-ary modulation scheme. Here convolutional code is concatenated with turbo code. Simulation result proves that as the M-ary value increases signal points increases which in turn supports high data rate. But at the same time the distance between the signal points comes closer which in turn reduces its immunity to noise.

Figure 7a shows the comparison between various orders of QAM modulation schemes. Here, the tag which is nothing but the pn sequence is embedded in the parity bits of the turbo code. Figure 7b shows the concatenated output. It shows that as the order of QAM increases data rate increases. But the energy spent in transmitting the bit increases when compared to 4-QAM and 16-QAM. Also when compared to the individual scheme the concatenated scheme offers good improvement in BER.

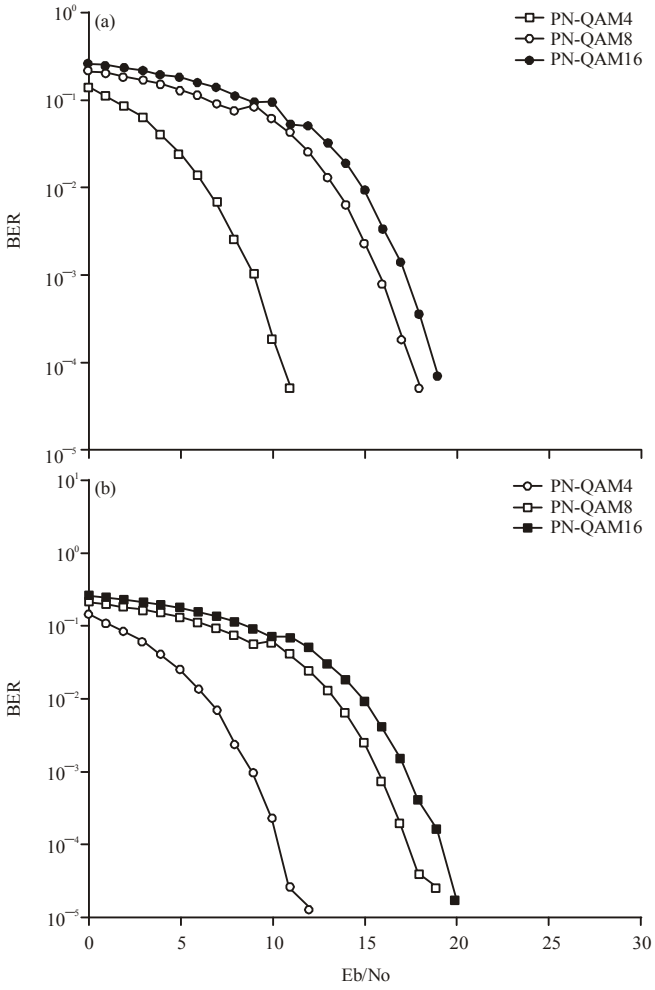

Fig. 7(a-b): PN sequence embedded in QAM, concatenated scheme, (a) PN turbo QAM and (b) PN with turbo covolution

CONCLUSION

This study focuses on mitigating the PUEA attack by embedding the tag in the parity bit of the error control code. The comparison between turbo and convolutional codes concluded that turbo code offer better result than convolutional code. The BER performance analysis of the system with turbo codes under various modulation schemes proved that BPSK is less error prone when compared to QAM. Also simulation results proved that turbo code when concatenated with convolutional code topped than the individual one because of the improved coding gain. Hence proper choice of error control code, modulation scheme and the number of tag bits embedded leads to a good fight against malicious users.

REFERENCES

Alahmadi, A., M. Abdelhakim, J. Ren and T. Li, 2014. Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. IEEE Trans. Inform. Forensics Secur., 9: 772-781.

Avila, J., E. Vinoth, E. Praveen and K. Thenmozhi, 2012. Performance augment of Multiband OFDM with ANN assisted concatenated codes. Proceedings of the IEEE International Conference on Computing, Electronics and Electrical Technologies, March 21-22, 2012, Kumaracoil, India, pp: 76-80.

Chen, R., J.M. Park and J.H. Reed, 2008. Defense against primary user emulation attacks in cognitive radio networks. IEEE J. Selected Areas Commun., 61: 25-37.

Haykin, S., 2005. Cognitive radio: Brain-empowered wireless communications. IEEE J. Sel. Areas Commun., 23: 201-220.

Holmes, J. and C. Chen, 1977. Acquisition time performance of PN spread-spectrum systems. IEEE Trans. Commun., 25: 778-784.

Hoshyar, R., S.H. Jamali and A.R.S. Bahai, 2000. Turbo coding performance in OFDM packet transmission. Proceedings of the IEEE 51st Vehicular Technology Conference, Volume 2, May 15-18, 2000, Tokyo, pp: 805-810.

Jin, Z., S. Anand and A. Subbalakshmi, 2009. Detecting primary user emulation attacks in dynamic spectrum access networks. Proceedings of the IEEE International Conference on Communications, June 14-18, 2009, Dresden, Germany, pp:1-5.

Kim, H.S., 2011. Location-based authentication protocol for first cognitive radio networking standard. J. Network Comput. Applic., 34: 1160-1167.

Kumar, S. and S. Sharma, 2007. Error probability of different modulation schemes for OFDM based WLAN standard IEEE 802.11a. Int. J. Eng., 4: 262-267.

Kumar, V., J.M. Park, J. Kim and A. Aziz, 2012. Physical layer authentication using controlled inter symbol interference. Proceedings of the IEEE International Symposium on Dynamic Spectrum Access Networks, October 16-19, 2012, Bellevue, WA., pp: 286-290.

Liu, Y., P. Ning and H. Dai, 2010. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. Proceedings of the IEEE Symposium on Security and Privacy, May 16-19, 2010, Oakland, CA., USA., pp: 286-301.

Mitola, J., 2000. Cognitive radio: An integrated architecture for software defined radio. Ph.D. Thesis, Royal Institute of Technology, Sweden.

Nomura, R., M. Kuroda and T. Mizuno, 2011. Radio-free mutual authentication for cognitive radio network. Inform. Media Technol., 62: 580-594.

Nyirongo, N., W.Q. Malik and D.J. Edwards, 2006. Concatenated RS-convolutional codes for ultrawideband multiband-OFDM. Proceedings of the IEEE International Conference on Ultra-Wideband, September 24-27, 2006, Waltham, MA., USA., pp: 137-142.

Parvin, S., S. Han, B. Tian and F.K. Hussain, 2010. Trust-based authentication for secure communication in cognitive radio networks. Proceedings of the IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing, December 11-13, 2010, Hong Kong, pp: 589-596.

Pu, D. and A.M. Wyglinski, 2014. Primary-user emulation detection using database-assisted frequency-domain action recognition. IEEE Trans. Vehicular Technol., 63: 4372-4382.

Salem, F.M., M.H. Ibrahim, I.A. Ali and I.I. Ibrahim, 2014. Matched-filter-based spectrum sensing for secure cognitive radio network communications. Int. J. Comput. Applic., 87: 41-46.

Sklar, B. and P.K. Ray, 2001. Digital Communications: Fundamentals and Applications. 2nd Edn., Pearson Education, USA.

Taheri, S., A. Sharifi and R. Berangi, 2012. Deal with attacks over cognitive radio networks authentication. Int. J. Comput. Technol. Applic., 3: 2027-2032.

Viraktamath, S.V. and G.V. Attimarad, 2010. Impact of constraint length on performance of convolutional CODEC in AWGN channel for image application. Int. J. Eng. Sci. Technol., 2: 4696-4700.

Ward, R.B., 1965. Acquisition of pseudonoise signals by sequential estimation. IEEE Trans. Commun. Technol., 13: 475-483.