Improving the Physical Layer Security of Wireless Communication Networks using Spread Spectrum Coding and Artificial Noise Approach

Kazeem Adedeji[*], Yskandar Hamam[*], Bolanle Abe[*] and Adnan Abu-Mahfouz[#]

[*]*Department of Electrical Engineering, Tshwane University of Technology, Pretoria, South Africa*

adedejikb@tut.ac.za, hamama@tut.ac.za, abebt@tut.ac.za

[#]*Council for Scientific and Industrial Research, Meraka Institute, Pretoria, South Africa*

aabumahfouz@csir.co.za

Abstract— **Recent advances in technologies has led to the use of wireless communication networks for the transmission of information. However, the broadcast nature of wireless channels has made it vulnerable to attacks. In this paper, we present work in progress on a proposed hybrid spread spectrum coding and artificial noise approach to improving the physical layer security of wireless communication channels. The authors are optimistic that, the proposed method will further improve the physical layer security of wireless communication networks.**

Keywords— **Physical layer security, secrecy capacity, spread spectrum, wireless channels.**

I. INTRODUCTION

The market for wireless communications over the years has enjoyed a tremendous growth, being applied to the realm of personal and business computing, military intelligence, medical information, government information and service providers. However, wireless communication networks are vulnerable to attack because of the open nature of wireless transmission. Most of the security techniques in wireless communication networks are based on the use of conventional cryptography based algorithm in the upper layer of the protocol stack [1]. A protocol layer is a technique for simplifying networking tasks, by dividing each task into functional layer's task. Fig. 1 shows the seven layers of open system interconnection (OSI) reference model in a typical wireless communication protocol. Each layer handles some specific functions and security solutions. Cryptography based encryption is performed at the application layer to protect the messages against eavesdropping. However, the evolution of strong deciphering mechanisms has made conventional cryptography-based security techniques ineffective against attacks from an intruder.

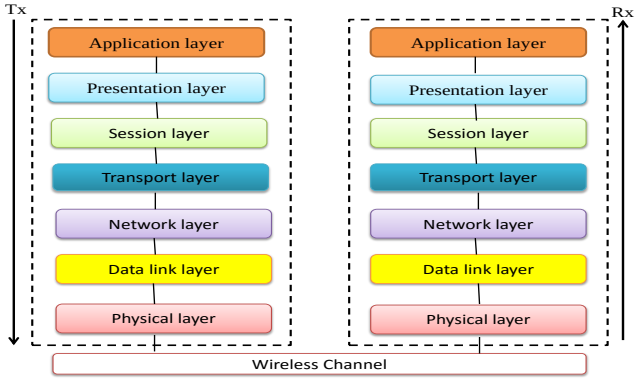

Figure 1: Layer protocol architecture

Research work in [2-5] has introduced a security technique complementing the conventional cryptography-based security and significantly improved the overall security of wireless communication networks. This leads to the current security mechanism called physical layer security. The physical layer security is an emerging security research area in wireless communication networks, which exploits the physical characteristics of the wireless medium to provide secure communication [3].

Numerous studies dealing with this problem have been published. The early studies of [4, 5] gave a first insight into the problem. More recently, the research works of [3,6-9] have shown that a positive information rate can be achieved under the information-theoretic secrecy requirements; meaning that a better secrecy capacity can be achieved if SNRs of the main channel is greater than that of the eavesdropper's channel. Other papers dealing with the physical layer security issues are reported in the literature, some of which include; jammer selection [10], and game theoretic approach [11].

In the current study, we proposed a hybrid spread spectrum coding and artificial noise approach for improving the physical layer security of wireless communication channels. The rest of the paper is organized accordingly. Section II deals with the research goal. In Section II, the proposed methodology for the study is presented while Section IV concludes the paper.

II. RESEARCH GOAL

The goal of the research study is to improve the physical layer security of wireless channels by employing a hybrid spread spectrum coding and artificial noise approach. Spread spectrum techniques can be deployed for security purpose due to its anti-jamming properties and low probability of intercept.

III. RESEARCH METHODOLOGY

The simplified block diagram of the proposed hybrid DSSSC-AN technique for improving the physical layer security of wireless communication networks is shown in Fig. 2.This system employs a direct sequence spread spectrum coding (DSSSC) and Artificial noise (AN) approaches to physical layer security. Considering the figure, *m(t)* denotes the message signal to be transmitted which will be passed into a DSSS to spread it over a wide range of frequencies using a PN code sequence. The output signal from this is modulated on a carrier frequency using BPSK modulation technique; being the most widely used modulation technique in spread spectrum

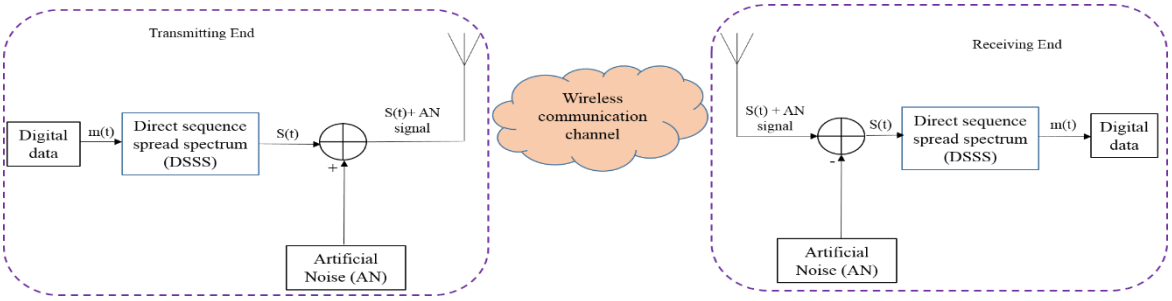

Figure 2: Block diagram of the proposed DSSS-AN physical layer security.

systems. The resulting signal after BPSK modulation gives the DSSS signal. Using a BPSK modulation technique, the resulting spread signal *S(t)* is given by

$$S(t)=\frac{\sqrt{2E}}{T}m(t)\,p(t)\cos(2\pi f_c t+\theta) \quad (1)$$

where E is the signal energy, T is the period, $p(t)$ is the PN spreading sequence signal, f_c is the carrier frequency of the modulation and θ is the phase angle of the carrier. The DSSS signal $S(t)$ is mixed with an artificial noise block and the resulting signal ($S(t)+An(t)$) is transmitted through a transmitting antenna at the sending end to a receiver over a wireless communication channel in the presence of eavesdroppers having a receiving antenna. The purpose of the $An(t)$ is to degrade the quality of the received signal at the eavesdroppers side by transmitting the artificial noise signal in all directions. The wireless communication channel will be modelled as AWGN channel. The receiving end consist of i^{th} number of receivers and eavesdroppers as shown in Fig. 3.

The signal that is received by the i^{th} legitimate receiver y_{Ri} and the eavesdroppers y_{Ei} are expressed as

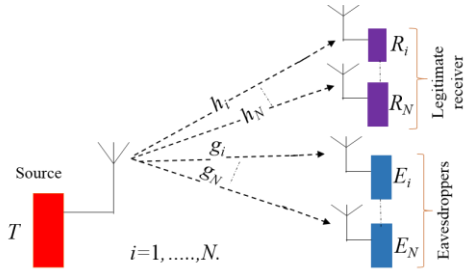

Figure 3: Representation of receiver and eavesdroppers antenna.

$$y_{R_i}=h_i S(t)+n_r(t) \quad (2)$$

$$y_{E_i}=g_i S(t)+n_e(t) \quad (3)$$

where h_i and g_i denote the gain of the legitimate and the eavesdroppers channel, between the transmitting end and the i^{th} legitimate receivers and eavesdroppers respectively. Also, n_r and n_e are the AWGN at the legitimate receiver and the eavesdropper's channel.

At the receiving side, the reverse process of this will be done. Also, the transmitting end and the receiving end must be synchronized, meaning that the same PN code used at the sending end for spreading the signal must also be used at the receiving end for de-spreading the signal after which a BPSK demodulation process will be performed on it to retrieve the original message signal. This system will be simulated in MATLAB/SIMULINK and its performance determine based on the secrecy capacity, the secrecy outage probability, and secrecy throughput.

IV. CONCLUSION

The security issues at the application layer of the protocol stack of wireless communication networks have been an emerging research area. Various approaches are being proposed to improve security issues in wireless networks. This work proposes a hybrid technique for solving security challenges over this network. The hybrid DSSSC-AN technique, expected to improve physical layer security of wireless communication networks.

ACKNOWLEDGMENT

This research work is supported by Tshwane University of Technology and the Council for Scientific and Industrial Research, Pretoria, South Africa.

REFERENCES

[1] C.B. Sankara, "Network access security in next generation 3GPP systems: a tutorial," *IEEE Communications Magazine*, vol. 47, no. 2, pp. 84-91, 2009.

[2] C.E. Shannon, "Communication theory of secrecy system," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[3] H.V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Communications*, vol. 19, no. 1, pp. 40-47, 2012.

[4] A.D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[5] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339-348, 1978.

[6] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515-2534, 2008.

[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communication*, vol. 7, pp. 2180-2189, 2008

[8] C. Arsenic, M.S. Perlaza, H. Zhu, H. Vincent, "Physical layer security in wireless communication networks with passive and active eavesdropper," *IEEE Globecom; Wireless Communication System*, pp. 4868-4873, 2012.

[9] Y. Zou, X. Wang and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099-2111, 2013.

[10] J. Chen, R. Zhang, L. Song, Z. Han and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, 2012, 310-320, 2012.

[11] M. Yuksel, X. Liu and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 818-830, 2011.

Kazeem Adedeji received his M.Eng and M.Tech in 2015 and 2016 respectively. He is currently doing his doctorate degree at Tshwane University of Technology, Pretoria, South Africa. His research area include data communication and network security, broadband communication and sensor networks.