Chapter 9
PSO-Based Antenna Pattern Synthesis: A Paradigm for Secured Data Communications

Rathindra Nath Biswas
Acharya Jagadish Chandra Bose Polytechnic, India

Anurup Saha
Jadavpur University, India

Swarup Kumar Mitra
MCKV Institute of Engineering, India

Mrinal Kanti Naskar
Jadavpur University, India

ABSTRACT

An antenna pattern synthesis scheme based on particle swarm optimization (PSO) technique is proposed. Synthesized patterns always contain narrower beamwidth and minimum side-lobes level reducing coverage areas towards the attackers in wireless networks. On such patterns, deep nulls are also steered at various interfering directions as to provide a second layer of protection. Using selective patterns at each point-to-point link, data privacy is ensured throughout entire route from source to sink. This approach is simple enough to be commensurate with flexible design methods on a real-time platform. Thus, an FSM (finite state machine) rule-based digital system model is further developed and tested on Xilinx Virtex4 FPGA (field programmable gate array) board. Its performance under harsh radio environmental conditions is also verified with several fixed-point simulations in terms of pattern synthesis accuracy and computational overheads. These results corroborate such system integration onto wireless infrastructures for the secured data communication services.

DOI: 10.4018/978-1-5225-5852-1.ch009

INTRODUCTION

Wireless technologies usually provide numerous potential benefits like enormous bandwidth, less space, light weight, ease of installation and maintenance etc. Obviously, these are also essential requirements for the design of state-of-the-art communication systems. However, a continuous research growth during the last decade makes it possible simply to develop low power and low cost wireless devices and circuits on both of MMIC (monolithic microwave integrated circuits) as well as VLSI (very large scale of integration) architecture. Thus, wireless systems utilizing radio frequency (RF) signals or microwaves and millimeter waves are now extensively used in various sectors of communication services (Schafer et al, 2014; Schafer, 2003). For implementation of long-haul communication systems, multi-hop networks are generally constituted with several wireless transceivers (transmitter-receiver) to relay the broadcast messages at the receiving end in a cooperative manner. During transmission and reception of RF signals, the transceivers (also termed as nodes) inevitably share a common channel in free space. Consequently, data communications among the nodes become vulnerable to the attackers mostly at the physical and other outer layers (Zhou et al, 2014; Zhou et al, 2016). At most of the cases, attackers appear in pretention of the benevolent nodes within the networks and normally get access to the control systems of few nodes using malicious codes to compromise them. They mislead the entire system operation by transferring erroneous information through the multi-hop data links (Khan et al, 2014; Mahmoud et al, 2014). Therefore, preserving privacy and security of data along its route from source to destination has turned into a prime issue in modern wireless communication systems. Several popular cryptographic methods were proposed so far and these work well for protecting data at the application and other inner layers. Nonetheless, only few approaches were adopted to defend the physical layer attacks (Wong et al, 2007; Wong et al, 2011). Besides, the task of implementing a secured data communication network with simple structure that must ensure data privacy over its radio links still puts a great challenge to the system designers. Hence, much more research attention is required to enrich both of its algorithmic and architectural attributes.

Adversaries are supposed to sustain their activities via few compromised nodes in the network and thus a continuous evaluation of trust-worthiness of each node is always necessary prior to all data forwarding steps. Antenna pattern synthesis, however, could guarantee safe data transfer to some extent within a harsh radio propagation environment (Mailoux, 2005; Hong et al, 2014). Unlike omnidirectional pattern, it concentrates most of its radiated power in a particular direction and thus improves gain and directivity of the antenna significantly. This strategic approach also enhances the channel capacity of wireless medium. The nodes of wireless networks usually require patterns with narrower beamwidth and lower side-lobes level so that interferences from their neighborhood cannot hamper data privacy in a particular link. In fact, it also optimizes throughput and latency in the systems, selecting an optimal route for relaying data packets from source to sink (Bagchi et al, 1999; Mishra, 2008). On the contrary, advanced communication systems such as mobile ad-hoc networks (MANET) or internet of things (IoT) based wireless local area networks (WLAN) etc. now utilize smart devices that enable them to estimate interfering directions in a more convenient way (Yang et al, 2004; Jiang et al, 2007; Ilyas et al, 2005). Therefore, pattern synthesis methods would be much more effective to counteract the attacks, steering deep and wide nulls against the interferers. However, the scheme becomes trickier enough to put up this additional criterion. Antenna operation rather can be made more ‘smart’ considering any particular array configuration (i.e., linear, circular or planar etc.) and computing its weight vectors in terms of element excitation coefficients or phases iteratively on a digital signal processor (DSP) to obtain the desired