IGI PUBLISHING **ITB14872**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **Web Services Security and E-Business**
edited by **G. Radhaman & G. S. V. Radha Krishna Rao © 2007, IGI Global**

Chapter II

Wireless Web Security Using a Neural Network-Based Cipher

Isaac Woungang, Ryerson University, Canada

Alireza Sadeghian, Ryerson University, Canada

Shuwei Wu, Ryerson University, Canada

Sudip Misra, Cornell University, USA

Maryam Arvandi, Ryerson University, Canada

Abstract

The increasingly important role of security for wireless Web services environments has opened an array of challenging problems centered on new methods and tools to improve existing data encryption and authentication techniques. Real-time recurrent neural networks offer an attractive approach to tackling such problems because of the high encryption capability provided by the structural hidden layers of such networks. In this chapter, a novel neural network-based symmetric cipher is proposed. This cipher releases the constraint on the length of the secret key to provide the data integrity and authentication services that can be used for securing wireless Web services communication. The proposed symmetric cipher design is robust in resisting different cryptanalysis attacks. Simulation results are presented to validate its effectiveness.

Introduction

With the widespread availability of the 802.11b standard and products, and their deployment in wireless networks supporting a host of telecommunication services, including multimedia services, there is a clear demand for network layer security, in recent years. In a wireless setting, any host within physical communications range can intercept and spoof network packets; therefore, corporate as well as wireless residential users face a substantial security threat. Resolving these problems at the application layer alone is not a desirable solution (Stubblefield et. al., 2002). For example, all applications would have to be upgraded on both the client and server sides to use authenticated protocols, which would take a considerable amount of time. However, network layer security protocols, such as the Internet protocol security (IPSec, 2004), provide the capability to solve these problems, since it secures end-to-end communications between hosts (Kent & Atkinson, 1998). As encryption is at the core of this framework, as well as many other security and authentication protocols, this chapter proposes a novel neural network-based symmetric cipher for message encryption. This novel cipher block chaining mode (CBC)-based encryption scheme is robust in resisting different cryptanalysis attacks, and provides efficient data integrity and authentication services that can be beneficial to wireless Web services. The design of the proposed symmetric cipher is presented, and its security is analyzed by examining two types of attacks: one against the message authentication code (MAC), and the other against the data encryption scheme itself. Simulation results are also presented to validate the effectiveness of the proposed symmetric cipher design.

The rest of the chapter is organized as follows. First, a background work sustaining the topic discussed in this chapter is presented as follows: (1) Cryptographic as a motivation for this study; (2) Review of previous research pertinent to applying neural network in cryptography. Second, the main thrusts of this chapter are discussed, which include (1) The proposed novel symmetric cipher design; (2) A security analysis of the proposed cipher design; and (3) Simulation results validating the proposed cipher design. Third, the future and emerging trends of the studied topic are discussed, which include a viability study, and foreseen research issues related to the aforementioned symmetric cipher design. Finally, the conclusion is presented.

Cryptography as a Motivation for this Study

The boundary of interaction between communicating systems has significantly increased from intranets to the Internet with the adoption of Web services. In this context, information security (understood here as authentication, access control, confidentiality, integrity, and nonrepudiation) has become a top priority due to the existence of threats such as viruses, hackers, electronic eavesdropping, frauds, and so forth. One way to protect the secrecy of the information is by using *cryptography*, known as the science