Chapter 4.1
A Survey on Applied Cryptography in Secure Mobile Ad Hoc Networks and Wireless Sensor Networks

Jianmin Chen
Florida Atlantic University, USA

Jie Wu
Florida Atlantic University, USA

ABSTRACT

Many secure mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs) use techniques of applied cryptography. Numerous security routing protocols and key management schemes have been designed based on public key infrastructure (PKI) and identity-based cryptography. Some of these security protocols are fully adapted to fit the limited power, storage, and CPUs of these networks. For example, one-way hash functions have been used to construct disposable secret keys instead of creating public/private keys for the public key infrastructure. In this survey of MANET and WSN applications we present many network security schemes using cryptographic techniques and give three case studies of popular designs.

INTRODUCTION

This chapter aims to explain how MANET and WSN security design may be improved with a broad knowledge of cryptography. Securing MANETs and WSNs requires consideration of the following factors: dynamic topologies, resource constraints, no infrastructure, and limited physical security. Because WSNs typically have more nodes and less power than MANETs, their security design requires more attention to computational capabilities and memory resources. Much

DOI: 10.4018/978-1-61350-101-6.ch401

cryptographic, authentication, and authorization research has been conducted into the details of secure routing, key management, and trust management in MANETs and WSNs.

Previous researches have studied attacks and countermeasures in MANETs (Wu & Chen, 2008), key management in MANETs (Wu & Cardei, 2008), security locations in WSNs (Srinivasan, 2008), secure routing protocols in MANETs (Pervaiz, 2008), challenges and solutions in wireless security (Lou, 2003), key management schemes in WSNs (Xiao, 2007), and open issues in WSNs (Evans, 2006). To increase network security cryptographic techniques may be applied in different areas of MANETs/WSNs. For example, ID-based cryptography (Shamir, 1984) is used to develop a new certificateless security scheme in MANETs as well as for a security scheme in vehicular ad hoc networks and for other secure routing applications. Case studies of cryptographic techniques in customized MANETs and WSNs will provide the research community with the latest updates in security and performance for MANETs and WSNs. One example of a new foundation for advanced research is a configurable library for elliptic curve cryptography in WSNs called TinyECC (Liu, 2008). Our survey is an effort to promote the use of cryptographic techniques in the ongoing research to better secure MANETs/WSNs.

Our case studies are chosen to discuss symmetric cryptography, public key infrastructure (PKI), identity-based cryptography, threshold cryptography, and batch verification of signatures. After summarizing cryptographic techniques we give an overview of commonly used security designs followed by sections on symmetric cryptographic techniques. Our discussion of the symmetric techniques is based on a case study of LHAP (Zhu & Xu, 2003). Our discussion of the asymmetric techniques, with a special emphasis on composite design, is based on a case study of IKM (Zhang, Liu, Lou & Fang, 2006). Then we discuss how threshold cryptography is used in different cases for secret sharing to make gains in both security and performance. Finally other cryptographic techniques are discussed on the basis of a case study of IBV by Zhang (Zhang, Lu, Ho & Shen, 2008) followed by our presentation of present open issues and future challenges.

CRYPTOGRAPHY TECHNIQUES OF SECURE MANETS/WSNS DESIGN

Security is the combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non-repudiation.

- **Confidentiality:** The confidentiality is to ensure that information is accessible only to those authorized users or nodes to have access. Since MANETs/WSNs use an open medium, all nodes within the direct transmission range can usually obtain the data. One way to keep information confidential is to encrypt the data. In WSNs confidentiality is employed to protect information from inadvertent disclosure while communicating between one sensor node and another sensor node or between the sensors and the base station. Compromised nodes are a threat to confidentiality if the cryptographic keys are not encrypted and stored in the node.
- **Authentication:** The goal of authentication is to identify a node or a user and to prevent impersonation. In wired networks and infrastructure-based wireless networks it is possible to implement a central authority at a router, base station, or access point. However, there is no central authority in MANETs/WSNs, and it is much more difficult to authenticate an entity. Confidentiality can be achieved via encryption. Authentication can be achieved by using a message authentication code (MAC) (Menezes, Oorschot & Vanstone, 1996).