Chapter XXX
A Survey of Key Management in Mobile Ad Hoc Networks

Bing Wu
Fayetteville State University, USA

Jie Wu
Florida Atlantic University, USA

Mihaela Cardei
Florida Atlantic University, USA

ABSTRACT

Security has become a primary concern in mobile ad hoc networks (MANETs). The characteristics of MANETs pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and nonrepudiation. Cryptographic techniques are widely used for secure communications in wired and wireless networks. Most cryptographic mechanisms, such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. However, all cryptographic techniques will be ineffective if the key management is weak. Key management is also a central component in MANET security. The purpose of key management is to provide secure procedures for handling cryptographic keying materials. The tasks of key management include key generation, key distribution, and key maintenance. Key maintenance includes the procedures for key storage, key update, key revocation, key archiving, and so forth. In MANETs, the computational load and complexity for key management are strongly subject to restriction by the node's available resources and the dynamic nature of network topology. A number of key management schemes have been proposed for MANETs. In this chapter, we present a survey of the research work on key management in MANETs according to recent literature.

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Mobile Ad Hoc Networks (MANETs)

In areas where there is little communication infrastructure or the existing infrastructure is inconvenient to use, wireless mobile users may still be able to communicate through the formation of *mobile ad hoc networks* (Perkins, 2001). A mobile ad hoc network, or simply MANET, is a collection of wireless mobile hosts that form a temporary network without the aid of any centralized administration or support. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may be multiple hops away from each other.

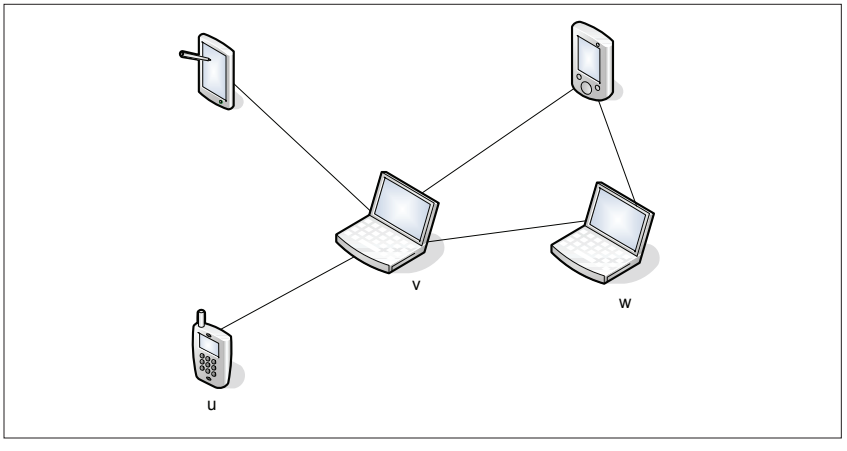
Possible applications of MANETs include: soldiers relaying information for situational awareness on the battlefield; business associates sharing information during a meeting; attendees using laptop computers to participate in an interactive conference; and emergency disaster relief personnel that are coordinating efforts at sites of fires, hurricanes, or earthquakes.

A routing protocol is necessary in such an environment, since two hosts that wish to communicate may not be able to exchange packets directly. Figure 1 shows a simple example of a MANET. Host *w* is not within the range of host *u*'s wireless transmitter and vice versa. If *u* and *w* wish to exchange packets, they may depend on the services of host *v* to forward packets for them because *v* is within the overlap between *u* and *w*'s transmission range. Although the number of hops for a host to reach another is likely to be small, the routing problem in a real MANET will still be complicated due to the inherent nonuniform propagation characteristics of wireless transmissions, and the highly dynamic topology of the networks.

Characteristics of MANETs

A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to an interface with a fixed network. Its nodes are equipped with wireless transmitters/receivers using antennas that may be omnidirectional (broadcast), highly directional (point-to-point), or some combination thereof. At a given time, the system can be viewed as a random graph due to the movement of the nodes and their transmitter/receiver coverage patterns, the transmission power levels, and the cochannel interference levels (Karygiannis & Owens, 2002; Ravi, Raghunathan, & Potlapally, 2002; Stallings, 2002). The network topology may change with time as the nodes move or adjust their transmission and reception parameters. Thus, ad hoc networks have several salient characteristics:

Figure 1. An example of a mobile ad hoc network



19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/survey-key-management-mobile-hoc/22065

Related Content

Conservation of Mobile Data and Usability Constraints
Rania Mokhtarand Rashid Saeed (2012). *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies (pp. 40-55).*
www.irma-international.org/chapter/conservation-mobile-data-usability-constraints/56295

A Network Traffic Prediction Model Based on Graph Neural Network in Software-Defined Networking
Guoyan Li, Yihui Shang, Yi Liuand Xiangru Zhou (2022). *International Journal of Information Security and Privacy (pp. 1-17).*
www.irma-international.org/article/a-network-traffic-prediction-model-based-on-graph-neural-network-in-software-defined-networking/309130

Network Anomalies Detection Approach Based on Weighted Voting
Sergey Sakulin, Alexander Alfimtsev, Konstantin Kvitchenko, Leonid Dobkacz, Yuri Kalginand Igor Lychkov (2022). *International Journal of Information Security and Privacy (pp. 1-17).*
www.irma-international.org/article/network-anomalies-detection-approach-based-on-weighted-voting/284050

Privacy Preserving Classification of Biomedical Data With Secure Removing of Duplicate Records
Boudheb Tarikand Elberrichi Zakaria (2021). *Research Anthology on Privatizing and Securing Data (pp. 569-588).*
www.irma-international.org/chapter/privacy-preserving-classification-of-biomedical-data-with-secure-removing-of-duplicate-records/280193

Cryptographic and Steganographic Approaches to Ensure Multimedia Information Security and Privacy
Ming Yang, Monica Trifas, Guillermo Francia IIIand Lei Chen (2009). *International Journal of Information Security and Privacy (pp. 37-54).*
www.irma-international.org/article/cryptographic-steganographic-approaches-ensure-multimedia/37582