Chapter 59

Secure Routing and Mobility in Future IP Networks

Kaj Grahn
Arcada University of Applied Sciences, Finland

Jonny Karlsson
Arcada University of Applied Sciences, Finland

Göran Pulkkis
Arcada University of Applied Sciences, Finland

ABSTRACT

The evolution of computer networking is moving from static wired networking towards wireless, mobile, infrastructureless, and ubiquitous networking. In next-generation computer networks, new mobility features such as, seamless roaming, vertical handover, and moving networks are introduced. Security is a major challenge in developing mobile and infrastructureless networks. Specific security threats in next-generation networks are related to the wireless access mediums, routing, and mobility features. The purpose of this chapter is to identify these threats, and discuss the state of the art of security research and standardization within the area. Proposed security architectures for mobile networking are presented. A survey of security in routing is provided with special focus on mobile ad hoc networks (MANETs). The security of currently relevant protocols for management or node and network mobility, Mobile IP (MIP), Network Mobility (NEMO), Mobile Internet Key Exchange (MOBIKE), Host Identity Protocol (HIP), Mobile Stream Control Transmission Protocol (mSCTP), Datagram Congestion Control Protocol (DCCP), and Session Initiation Protocol (SIP), is described.

INTRODUCTION

In mobile networking two fundamental features require new security solutions. The first fundamental feature is that the network infrastructure is no longer fixed. Home network protection can therefore no longer rely on network border defense, such as network traffic control in network gateways, since network borders can no longer be defined. Moreover, authentication and authorization solutions can no longer be based on network host location, for example defined by an IP address, since network host location changes cannot be predicted.

The second fundamental feature requiring new security solutions is the presence of wireless links in mobile networks. Secure communication in mobile networks can therefore no longer be based on protection and isolation of the communication media. The wireless links in mobile networks are not only end user node connections to the network. Also an entire network, for example a wired or wireless network in a train, can have changing wireless attachments to other networks. A network with a fixed structure to which mobile nodes and/or mobile networks are attached is called a *mobile infrastructure network*. Another mobile network type is a *mobile ad hoc network* (MANET) in which all network links are both wireless and changing.

This book chapter is a state of the art survey of

- security requirements,
- security architecture,
- routing security, and
- security of mobility management protocols

in present and future mobile networks.

SECURITY REQUIREMENTS IN MOBILE NETWORKS

Security is of most important concern when providing Internet mobility support. Any mobility solution must provide protection itself against attacks on and misuses of mobility features and mechanisms. Examples are stealing of legitimate addresses and flooding a node with a large amount of unwanted traffic. Complete and useful Internet mobility should address the security issues.

The following security requirements for a mobile infrastructure network type called 4G mobile networks with mobile end user devices are proposed in (Zheng et al., 2005), when end user devices called Mobile Equipment (ME) have location mobility and USIMs (Universal Subscriber Identity Module) as security modules:

1. Security requirements on an ME/USIM:
   - It shall protect the integrity of the hardware, software and OS in the mobile platform
   - It shall control access to data in ME/USIM.
   - It shall ensure confidentiality and integrity of data stored in the ME/USIM or transported on the interface between ME and USIM.
   - It shall retain user's identity as privacy to ME.
   - It shall prevent the stolen/compromised ME/USIM from being abused and/or used as an attack tool.
2. Security requirements on radio interface and network operator:
   - Entity authentication: mutual authentication between user and network shall be implemented to ensure secure service access and provision.
   - Ensure confidentiality of data including user traffic and signaling data on wired or wireless interface.
   - Ensure integrity and origin authentication of user traffic, signaling data and control data.
   - Security of user identity: It shall protect user identity confidentiality, protect user location confidentiality and prevent user traceability.
   - Lawful interception: It shall be possible for law enforcement agencies to monitor and intercept every call in accordance with national laws.
3. Security visibility, configurability and scalability:
   - The security features of the visited network should be transparent to the user.
   - The user can negotiate acceptable security lever with the visited network when user roams outside HE (home environment).

Related Content

Content-Based Image Retrieval Using Shape Features
(2018). *Image Retrieval and Analysis Using Text and Fuzzy Shape Features: Emerging Research and Opportunities (pp. 39-61).*
www.irma-international.org/chapter/content-based-image-retrieval-using-shape-features/195803

An Image Clustering and Feedback-based Retrieval Framework
Chengcui Zhang, Liping Zhou, Wen Wan, Jeffrey Birchand Wei-Bang Chen (2010). *International Journal of Multimedia Data Engineering and Management (pp. 55-74).*
www.irma-international.org/article/image-clustering-feedback-based-retrieval/40985

Design and Implementation of a Mobile and Portable Lifelog Media System
Baud Haryo Prananto (2009). *Handbook of Research on Mobile Multimedia, Second Edition (pp. 718-729).*
www.irma-international.org/chapter/design-implementation-mobile-portable-lifelog/21040

IP Video Surveillance System
(2014). *Video Surveillance Techniques and Technologies (pp. 264-289).*
www.irma-international.org/chapter/ip-video-surveillance-system/94146

Applying Machine Learning in Optical Music Recognition of Numbered Music Notation
Fu-Hai Frank Wu (2017). *International Journal of Multimedia Data Engineering and Management (pp. 21-41).*
www.irma-international.org/article/applying-machine-learning-in-optical-music-recognition-of-numbered-music-notation/182649