Chapter 17

QoS Signaling Security in Mobile Ad Hoc Networks

Ohm Sornil
National Institute of Development Administration, Thailand

ABSTRACT

A quality of service (QoS) signaling system is necessary for QoS provision in a mobile ad hoc network (MANET). A QoS signaling system in MANETs is vulnerable to various types of attacks, ranging from fabrication and modification of messages to denial of services, which can cause failures of QoS provisions. Security is thus a critical issue for a signaling system. However, distinctive characteristics of MANETs make security mechanisms effective in conventional networks inapplicable in this environment. This chapter describes issues and challenges, and examines mechanisms specifically designed to provide security for QoS signaling systems in MANETs.

INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a network of mobile nodes such as laptops and PDAs, connected via a wireless medium with no fixed infrastructure, e.g., wireless access point or router. This type of wireless network has become increasingly popular due to several advantages, including infrastructure-lessness, dynamical self-organization, self-adaptation, self-healing, robustness, and scalability (Marwaha et al., 2008). MANETs are suitable for a variety of applications (Reinsich et al., 2007; Toh, 2007), such as public safety, military, intelligent transportation, metropolitan area networks, building automation, as well as providing wireless network coverage to remote and inaccessible areas. Quality of service (QoS) is a set of bounds, such as latency, jitter, throughput, and packet loss to be maintained by the network for a particular data flow (Crawley et al., 1998). With the emergence of real-time applications such as Voice over Internet Protocol (VoIP) and video streaming, e.g., Video on Demand (VoD), strict QoS supports are required.

To provide QoS in a MANET, a signaling protocol is required to search for routes with sufficient resources for the desired QoS, to reserve and release

DOI: 10.4018/978-1-61520-791-6.ch017
resources, to set up, tear down, and renegotiate flows in the networks. Various types of attacks on a signaling protocol are possible such as signaling message fabrication, interception of QoS requests, modifications of QoS parameters, etc. Security is thus a critical aspect for the signaling system. Security properties that should be supported for QoS signaling systems in MANETs include confidentiality, availability, authenticity, integrity, and non-repudiation. Confidentiality requires the secrecy of the communication to be protected. Availability requires that services are available to an authorized entity. Authenticity ensures that an entity is who it claims to be. Integrity ensures that a message transmitted is not maliciously altered, and non-repudiation ensures that a node transmitting a message cannot deny the transmission.

Characteristics of MANETs, such as absence of fixed infrastructure, rapid topology change, high node mobility, and limited node capability, impose difficulties on security protection. Current approaches proposed for intrusion detection and security prevention on QoS signaling in wired networks (such as SDS/CD (Wu et al., 1999) and RSVP-SQOS (Talwar et al., 2001)) cannot be applied to MANETs, and new security techniques are necessary. Cryptographic mechanisms by themselves can only address a subset of security problems that exist with current QoS signaling. While attacks on routing generally focus on disrupting network connectivity, attacks on QoS signaling can affect routes established by secure routing protocols (Lu & Pooch, 2005). Without proper protection from security mechanisms, attacks on a QoS signaling system could result in QoS routing malfunction, interference of resource reservation, or even failure of QoS provision.

This chapter describes issues and challenges, and examines the state of the art in QoS signaling security in MANETs. The rest of the chapter is organized as follows. Section 2 discusses security issues in QoS signaling systems. Section 3 describes and analyzes two prominent security mechanisms specifically designed to protect QoS signaling systems. Section 4 provides concluding remarks.

**VULNERABILITIES AND ATTACKS ON QoS SIGNALING SYSTEMS IN MANETS**

**QoS Signaling Systems in MANETs**

A signaling protocol is required to propagate QoS reservation messages and establish appropriate QoS reservations. Two main QoS provisioning models in the Internet have been developed by IETF: Integrated Services (IntServ) (Braden et al., 1994) and Differentiated Services (Blake et al., 2009). The stateful IntServ, which maintains per-flow reservation state at QoS network entities, has a greater level of accuracy at a finer level of granularity. The stateless DiffServ does not maintain per-flow reservation state at QoS network entities and only relies on coarse classification and differential treatment of traffic. The two models are also adopted to provisioning QoS in MANETs. A number of QoS signaling protocols have been proposed for MANETs, for example, INSIGNIA, QoS AODV, SWAN, etc. (Chen & Nahrstedt, 1998)

In-Band Signaling System for Supporting QoS in MANET (INSIGNIA) (Lee et al., 2000) employs the option part of every IP packet to carry the signaling control. It is a per-flow based protocol (the IntServ approach) where the state of each flow is managed individually over a session in response to topology and end-to-end QoS condition changes. INSIGNIA uses a soft-state method to maintain its state information. Bandwidth is allocated to a particular flow if the QoS resource requirements of that flow can be satisfied. Otherwise, if the required resources are not available, the flow will be downgraded to a best-effort service. To be able to respond quickly to topology changes and varying end-to-end QoS conditions, INSIGNIA
Related Content

Medium Access Protocols for Cooperative Collision Avoidance in Vehicular Ad-Hoc Networks
[www.igi-global.com/chapter/medium-access-protocols-cooperative-collision/43167?camid=4v1a](www.igi-global.com/chapter/medium-access-protocols-cooperative-collision/43167?camid=4v1a)

Cryptographic Hash Function: A High Level View
[www.igi-global.com/chapter/cryptographic-hash-function/127155?camid=4v1a](www.igi-global.com/chapter/cryptographic-hash-function/127155?camid=4v1a)

Simulation of Multihop Wireless Networks in OMNeT++
[www.igi-global.com/chapter/simulation-multihop-wireless-networks-omnet/63282?camid=4v1a](www.igi-global.com/chapter/simulation-multihop-wireless-networks-omnet/63282?camid=4v1a)

Network Planning Algorithms for Optimizing Signalling Load in Mobile Networks
Vilmos Simon (2009). *Breakthrough Perspectives in Network and Data Communications Security, Design and Applications* (pp. 139-153).
[www.igi-global.com/chapter/network-planning-algorithms-optimizing-signalling/5938?camid=4v1a](www.igi-global.com/chapter/network-planning-algorithms-optimizing-signalling/5938?camid=4v1a)