Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Efficient authentication for fast handover in wireless mesh networks

Celia Li[*], *Uyen Trang Nguyen*, *Hoang Lan Nguyen*, *Nurul Huda*

Department of Computer Science & Engineering, York University, 4700 Keele Street, Toronto, Ontario, Canada M3J 1P3

ARTICLE INFO

Article history:
Received 21 September 2012
Received in revised form
3 June 2013
Accepted 10 June 2013

Keywords:
Wireless mesh networks
Network security
Authentication
Mobile devices
Hand-over
Hand-off
Key management
Privacy

ABSTRACT

We propose new authentication protocols to support fast handover in IEEE 802.11-based wireless mesh networks. The authentication server does not need to be involved in the handover authentication process. Instead, mesh access points directly authenticate mobile clients using tickets, avoiding multi-hop wireless communications in order to minimize the authentication delay. Numerical analysis and simulation results show that the proposed handover authentication protocol significantly outperforms IEEE 802.11 authentication in terms of authentication delay.

1. Introduction

A wireless mesh network (WMN) consists of mesh clients and mesh points (routers). Mesh clients can be static (e.g., desktops, database servers) or mobile hosts (e.g., cell phone, laptops, PDAs). The MPs form a wireless mesh backbone to provide multi-hop connectivity from one mesh client to another or to the Internet. A subset of mesh points act as *mesh access points* (MAPs), connecting mesh clients to the WMN. A small number of mesh points work as gateways, connecting the WMN to the Internet.

A WMN is dynamically self-organized and self-configured, with nodes in the network automatically establishing and maintaining mesh connectivity among themselves. This feature brings many benefits to IEEE 802.11-based mesh networks such as low installation cost, large-scale deployment, fault-tolerance, and self-management.

Wireless mesh networks support many important applications such as Internet access provisioning in rural areas, ad hoc networking for emergency and disaster recovery, security surveillance, and information services in public transportation systems, airports, shopping malls, and stadiums. The technology enables networking capability where wiring or installing cables is difficult or expensive and deployment time is a concern.

With the rapid growth of mobile services for handheld devices such as smartphones, tablets and laptops, Internet connectivity anytime anywhere has become a necessity in every day life, business, education and entertainment. While cellular networks effectively handle the handoff problem

[*] *Corresponding author.*
E-mail addresses: cli@cse.yorku.ca (C. Li), utn@cse.yorku.ca (U.T. Nguyen), lan@cse.yorku.ca (H.L. Nguyen), huda@cse.yorku.ca (N. Huda).

0167-4048/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2013.06.001

using signaling embedded in their low-level protocols, there are currently no efficient, transparent handoff solutions for IEEE 802.11-based wireless networks. At the moment, these networks, even if they give the appearance of continuous connectivity to a roaming client, provide connections that are in fact often interrupted when a client transfers from one access point to the next, because handover delays can be as long as several seconds (Velayos and Karlsson, 2003). For some applications (e.g. transferring files), this delay is acceptable; however, it is far too long for real-time traffic such as interactive voice over IP or video conferencing (Amir and Danilov, 2006).

The current version of wireless mesh networking standards IEEE 802.11s does not specify any mechanisms to support fast hand-off for mobile clients. A mesh client has to be authenticated by an authentication server via *multi-hop wireless communications*, which may result in long delay, low reliability and thus potential service interruption. A performance study of message transmission delay in IEEE 802.11-based mesh networks by Srivatsa and Xie (2008) shows that as the number of wireless hops between two routers increases from one to five, the delay of a message between a client and an authentication server increases from 0.15 s to 0.8 s. Since the authentication process involves several messages (e.g., nine messages in the EAP-TLS protocol used by 802.11s), the handoff latency may be several seconds long, which is not tolerable in real-time applications such as VoIP, newscast, and stock quote distribution.

Our work in this paper contributes toward extending the IEEE 802.11s standards to support fast roaming for mobile clients. In particular, we focus on fast authentication during the hand-off process as well as during the initial login time. We propose a new trust model for WMNs based upon which our proposed authentication protocols are designed. We present ticket-based authentication protocols that are efficient and resilient to attacks. The authentication server does not need to be involved in the handover authentication. Instead, mobile clients' authentications are done by mesh access points, avoiding multi-hop wireless communications. Fast authentication from one MAP to another during the hand-off process is supported using tickets (Kohl and Neuman, 1993). Numerical analysis and simulation results show that our login authentication protocol improves the latency of 802.11s login authentication, and our handover authentication protocol supports fast authentication during the hand-off process, which is lacking in 802.11s.

The remainder of the paper is organized as follows. Related work is discussed in Section 2. We describe the ticket types used in the proposed authentication protocols in Section 3. In Section 4, we present our login and handover authentication protocols. Security analysis is discussed in Section 5. Performance evaluations of the proposed protocols are given in Section 6. Section 7 concludes the paper and outlines our future work.

2. Related work

We first identify the requirements of an authentication protocol designed specifically for WMNs.

- The protocol must incur low computation costs due to mobile devices' limited computational capabilities, storage and/or power supply. The number of messages to be exchanged should be minimized due to the low bandwidth of wireless channels (compared with wired networks).
- The delay of re-authentication during the hand-off process should be low to avoid service interruption.
- The protocol must support mutual authentication between a client and a MAP, protection of client identity privacy, and resilient to various types of attacks (Horn et al., 2002) such as forgery, replay attack, denial of service attack, time-memory trade-off attack, and identity privacy attack. (These types of attacks will be defined and discussed in Section 5.)
- The amount of control traffic generated by mobility management mechanisms, such as handover authentication, has a significant impact on the overall network performance. Network operators are interested in reducing the amount of control traffic in their networks (possibly at the expense of higher server loads or lower handover performance (Kassab, 2007)).

We broadly divide authentication protocols for *wireless networks* in standards and in literature into three categories: multi-hop authentication, pro-active authentication, and ticket-based authentication. In multi-hop authentication protocols (IEEE, 2003; Forsberg et al., 2008; Jiang et al., 2006; Buddhikot, 2003; Shi, 2007), when a mobile client moves from one access point (network) to another, it has to be re-authenticated by the authentication server (home network) which may be located many hops away from the client. *Multi-hop wireless* communications incur long latency and may lead to service interruptions. Pro-active authentication protocols (Mishra et al., 2004; Park et al., 2007) attempt to minimize the authentication latency during the handover process by distributing pairwise master keys (PMK), proofs of successful log-in authentications, to potential target access points of a mobile client before the client moves to another access point. Ticket-based authentication protocols (Kassab, 2007; Li, 2010) also try to minimize the authentication latency during the handover process by using tickets as proofs of successful log-in authentications.

Pro-active and ticket-based authentication protocols follow the principles of single sign-on. They both execute login authentication one time and then calculate a PMK shared by a mobile client and a nearby access point. With the knowledge of the PMK, a client can be connected to that access point and authenticated quickly in the future.

2.1. *Multi-hop authentication*

The current wireless mesh networking standard IEEE 802.11s (IEEE, 2009; Hiertz, 2010) uses IEEE 802.11i security standards (IEEE, 2003). Using IEEE 802.11i login authentication protocol, such as EAP-TLS, a client is authenticated by an authentication server (AS), which may be many hops away from the client. When the client transfers from one MAP to another, he/she has to be re-authenticated by the AS, which incurs long latency.

IEEE 802.11F or Inter-Access Point Protocol (IAPP) is an optional extension to IEEE 802.11 that provides wireless access