Computer Networks 73 (2014) 185–194

Contents lists available at ScienceDirect

Computer Networks

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

Ticket-based handoff authentication for wireless mesh networks [☆,☆☆]

Li Xu [a,b,*], Yuan He [a], Xiaofeng Chen [c], Xinyi Huang [a]

[a] *Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350108, China*

[b] *Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, China*

[c] *State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an 710071, China*

ARTICLE INFO

Article history:
Received 8 August 2013
Received in revised form 10 April 2014
Accepted 8 August 2014
Available online 26 August 2014

Keywords:
Fast handoff
Re-authentication
Ticket
Lightweight
Wireless mesh networks

ABSTRACT

Due to the convenience of deployment and maintenance, wireless mesh networks (*WMNs*) have emerged as key techniques to support large-scale wireless coverage in both industrial and academic fields. Secure and seamless handoff is important to support mobility in *WMNs*. There are many existing works can be adopted to reduce the handoff latency, However, all these schemes require modifications to the original authentication protocols (e.g., different key architectures or trust relationships). In this paper, we propose a design based on ticket to achieve fast and secure handoff in *WMNs*. By pre-distributing the tickets to mesh client, the mesh client and the target mesh router can authenticate each other and establish temporary connection. Our scheme can be regarded as a supplementary specialized for handoff in *WMNs*, and no modification is required to the IEEE 802.1x authentication architecture. We achieve seamless handoff by using symmetric key operations and eliminating the involvement of a third party, which significantly reduces the computation and communication overheads. The security and performance analysis shows that our scheme is efficient in terms of security, computation overhead and handoff latency.

1. Introduction

Wireless mesh networks (*WMNs*) are designed to provide wireless access for mobile users. Compared with conventional wireless networks, *WMNs* have many distinctive features [1]:

1. *Multi-hop wireless network. WMNs* extend the coverage of wireless networks to non-line-of-sight distance by multi-hopping.
2. *Capability of self-forming, self-healing and self-organization.* Network performance can be improved dramatically due to flexible network architecture, easy deployment and configuration, fault tolerance, and multipoint-to-multipoint communications.

[☆] This article is a collaborative effort.

[☆☆] This work is supported by National Natural Science Foundation of China (Grant Nos. 61072080, 61202450, 61202452), Ph.D. Programs Foundation of Ministry of Education of China (Grant No. 20123503120001), Fok Ying Tung Education Foundation (No. 141065), Fujian Normal University Innovative Research Team (No. IRTL1207), Distinguished Young Scholars Fund of Department of Education, Fujian Province, China (JA13062), Department of Education, Fujian Province, A-Class Project (Grant No. JA12076), the development project of Fujian provincial strategic emerging industries technologies: Key technologies in development of next generation Integrated High Performance Gateway, Fujian development and reform commission high-technical (2013)266, and the open research fund of Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education.

[*] Corresponding author at: Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350108, China.

E-mail address: xuli@fjnu.edu.cn (L. Xu).

http://dx.doi.org/10.1016/j.comnet.2014.08.009
1389-1286/© 2014 Elsevier B.V. All rights reserved.

3. *Multiple types of network access. WMNs* support Peer-to-Peer communications, access to the Internet, and the integration with other wireless networks simultaneously.
4. *Compatibility and interoperability with existing wireless networks.* A *WMN* can be inter-operable with *WiMAX*, *ZigBee* and cellular networks, which support access for both mesh capable clients and conventional wireless clients.

Due to these merits, *WMNs* have emerged for a variety of applications in enterprise, community, metropolitan area networks, etc. They are regarded as one of the most promising backhaul techniques (that provide connectivity to the Internet backbone).

1.1. Architecture of a WMN

As we can see in Fig. 1, there are two kinds of nodes in a hybrid *WMN*: mesh routers (*MRs*) and mesh clients (*MCs*). *MRs* are usually stationary wireless devices and have no "constraint" on energy, computation and communication resources (compared with *MCs*). *MRs* provide wireless access and relay packets for *MCs* through multi-hop communication. Equipped with multiple wireless interfaces, *MRs* use the bandwidth and communicate with each other in an optimized way. *MRs* form the backbone of *WMNs* (infrastructure) and provide a non-line-of-sight coverage with much lower transmission power than conventional wireless networks. They contain proper routing protocols to balance the network load and offer a fair wireless service. When the access to the Internet is needed, some of them can serve as Internet gateways. *MCs* can be either conventional terminal equipments or devices capable of mesh functions. They can communicate with *MRs* as long as the same radio techniques are used. Being battery operated, *MCs* can achieve the mobility at a higher level. However, this requires that operations performed on *MCs* must be energy efficient.

Before a user obtains access to a *WMN*, it must perform mutual authentication with the corresponding access *MR* to make sure that both are legitimate entities. A successful authentication must satisfy three basic requirements: (1) *Authenticity*. The validity of the user and the access *MR* can be proved; (2) *Accessibility*. The valid user can be authorized the access to the network; (3) *Integrity*. The data transmitted within the network can be protected (not been tampered with, replayed and delayed maliciously). These objectives should also be guaranteed during handoff.

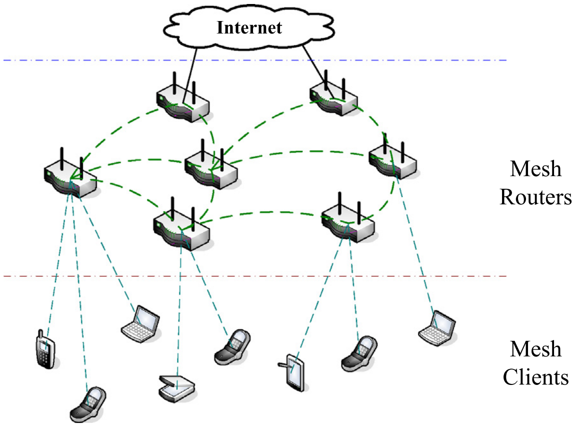

Fig. 1. Network model of a *WMN*.

1.2. Handoff in WMNs

Due to users' mobility in *WMNs*, *MCs* need to change their current access *MR* to a new one. When an *MC* moves to the serving boundary of its current connecting *MR*, the signal-to-noise ratio will fall due to signal attenuation. When it drops to a predetermined value, the *MC* will have to find a new *MR* for a better wireless service, which triggers handoff. We divide a handoff procedure into two phases: **probe** and **re-authentication**.

In the **probe** phase, an *MC* needs to scan all the channels successively to find an *MR* with the best signal quality to connect to. The issue of probe latency depends on the number of the available channels. Schemes in [2–4] can be adopted to easy this problem.

The purpose of the **re-authentication** phase is the same as that of authentication. This phase is affected by many different factors: congestion, the distance from the authentication server, the number of authentication message exchanges, etc. *MCs* need to perform key materials derivation and establish trust relationship with the new *MR*. Besides, *MRs* related to the roaming *MC* need to exchange frames about the quality of service (*QoS*), communication context, etc. As a result, re-authentication will cause a long latency which could not be acceptable for a realtime application. We focus on the reduction of re-authentication latency in this paper. There are several issues in handoff that deserve special attention [1]:

1. *Multi-hop wireless authentication.* In a three-party handoff protocol, authentication flows may need to travel through multiple wireless hops on both wired and wireless links, which will further increase the latency. It would be desirable if message exchanges are carried out only between two entities during handoff.
2. *Power constraints.* Mesh routers are capable for complex calculations and communications, while mesh clients are often power limited to support mobility. Mesh routers should carry most resource consuming operations to easy the burden of mesh clients.
3. *Cooperation feature.* Mesh routers relay packets for clients in a cooperative way. That means a roaming client can still connect to the previous access router by using the new router as a relay after handoff. In this case, a full authentication between the new router and the client is not necessary.

With these issues in mind, we design an efficient seamless handoff scheme for *WMNs* without any modifications on the original authentication protocol.

1.3. Motivation and our contributions

A number of schemes (e.g., [5–19]) have been proposed to cut down handoff latency. These schemes can be classi-