Computers and Electrical Engineering 000 (2016) 1–13

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A trustworthy and energy-aware routing protocol in software-defined wireless mesh networks☆

Hui Lin[a], Jia Hu[b,*], Li Xu[a], YouLiang Tian[c], Lei Liu[d], Stewart Blakeway[e]

[a] Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007 China
[b] Department of Mathematics and Computer Science, University of Exeter, Exeter EX4 4QF, UK
[c] College of Science, Guizhou University, Guiyang 550025, China
[d] School of Computer Science and Technology, Shandong University, Jinan 250100, China
[e] Department of Mathematics and Computer Science, Liverpool Hope University, Liverpool, L16 9JD, UK

ARTICLE INFO

Article history:
Received 1 February 2016
Revised 23 October 2016
Accepted 24 October 2016
Available online xxx

Keywords:
Hybrid wireless mesh networks
Privacy protection
Energy efficiency
Secure routing
Software defined networks

ABSTRACT

Hybrid Wireless Mesh Networks (HWMNs) were proposed to address the challenges in wireless communications to support mobile applications across different domains. Due to the multi-hop and decentralized network architecture, HWMNs are naturally susceptible to various security threats, especially internal attacks. Therefore, HWMNs must be able to detect anomalies, provide secure routing and protect user privacy through the cooperation among nodes. However, the existing routing protocols for HWMNs cannot ensure the security to protect the users privacy effectively. Moreover, traditional HWMNs are vertically integrated where the control and data planes of mesh routers are bundled together, which makes it complex and difficult to configure the network according to predefined security policies, and to adaptively respond to various dynamic security threats. Software-Defined Wireless Mesh Networks decouple the control plane and data plane of routers and thus enable a more flexible and efficient configuration of security policies. Taking up this opportunity to address the aforementioned challenges, this paper proposes a privacy-aware, secure and energy-aware green routing (PSGR) protocol that can defend against internal attacks, achieve stronger privacy protection and reduce energy consumption in Software-Defined HWMNs. The elaborate theoretical analysis verify that the PSGR protocol can implement the security and privacy protection against internal attacks effectively and efficiently. Simulation results demonstrate a superior performance of PSGR in terms of packet delivery ratio, network throughput and energy efficiency compared to the existing PA-SHWMP, PASER, and HWMP protocols in the presence of Blackhole/Grayhole attacks and wormhole attacks.

1. Introduction

The hybrid wireless mesh networks (HWMNs) integrate both ad hoc and backbone WMNs [1,2]. Due to the multi-hop decentralized architecture and special characteristics of the communication mode, HWMNs are exposed to various attacks, especially internal attacks launched by the internal legitimate nodes [2,3]. As a result, HWMNs face multiple threats

☆ Reviews processed and approved for publication by Editor-in-Chief.

* Corresponding author.
E-mail address: jiahu9@gmail.com (J. Hu).

http://dx.doi.org/10.1016/j.compeleceng.2016.10.015
0045-7906/

that could launch various internal attacks to obtain private data. Moreover, as the popularization and application scope of HWMNs expand unceasingly, more and more private information is stored in HWMNs. The leakage of such private information could bring disaster to individuals and the society. Consequently, internal attacks have become one of the most notable security problems in HWMNs [3].

As a fundamental and critical security aspect of HWMNs, the routing protocol has always been the main target of internal attacks. Various routing attacks launched from inside can damage the integrity, confidentiality and usability of private information [4]. Therefore, in order to achieve the protection of privacy and offer support for real-time applications and smooth delivery of broadband services, HWMNs must be equipped with a secure, privacy-aware and efficient routing protocol. Traditional HWMNs are vertically integrated where the control and data planes are bundled together, which makes the development and deployment of new routing algorithms very hard since it would imply a modification of the control plane of all network devices – through the installation of new firmware and, in some cases, hardware upgrades. However, Software-Defined Mesh Networks [5,6] decouple the control plane and data plane of mesh routers, thus enable a more flexible and efficient configuration of security policies in the secure routing protocols.

The implementation of a privacy aware secure routing protocol in Software Defined HWMNs is very challenging because of the following reasons: (1) The existing HWMP routing protocols introduced in HWMNs [7,8] are dependent on the cooperation of nodes and based on the assumption that the participating nodes are honest and well-behaved with no malicious or dishonest intentions. However, in practice nodes in a HWMN may be compromised by malicious users and are subject to various attacks from inside due to the intrinsically open and distributed nature of HWMNs [7]. (2) The mesh clients in the HWMNs could be mobile and thus are normally power constrained [8]. Therefore it is natural and imperative to consider the energy consumption of the mesh clients in routing so as to improve energy efficiency and thus prolong the battery life of the mesh clients.

To address the aforementioned issues, we propose a privacy-aware, secure and green routing protocol (PSGR) in HWMNs. In addition to achieving strong security and privacy protection, the PSGR can also maintain a good balance between security and performance. The major contributions of this work include:

(1) The proposed PSGR protocol integrates a novel dynamic reputation mechanism, a security level (SL) classified scheme and a hierarchical key management protocol in order to dynamically identify and manage the malicious nodes as well as defend against internal attacks in the routing process for HWMNs.
(2) The PSGR can further enhance privacy and security by preventing malicious nodes from modifying and interpreting packets. The energy consumption in PSGR is taken into account in the process of routing through the presented energy consumption analysis model which makes the PSGR satisfy the requirements of both security and energy-efficiency.
(3) Verified by the elaborate theoretical analyses, the PSGR protocol can implement the security and privacy protection against internal attacks effectively and efficiently. Extensive OPNET simulation experiments demonstrate that the PSGR protocol outperforms the existing routing protocols in terms of packet delivery ratio, network throughput and energy efficiency in the presence of Blackhole/Grayhole attacks and wormhole attacks.

The rest of the paper is organized as follows Section 2 presents a brief review of the related work; Section 3 describes the security, adversary and energy models; Sections 4 and 5 present the dynamic reputation mechanism and the PSGR routing protocol, respectively. Section 6 discusses the security and performance of PSGR. Finally, Section 7 concludes the paper.

2. Related work

The multi-hop decentralized architecture of HWMNs makes it difficult to design a privacy aware secure routing protocol. The early studies were devoted to applying ad hoc routing protocols for WMNs. However, due to the significant differences in the characteristics between ad hoc networks and WMNs such efforts were not fruitful [9].

Afterwards, tremendous research has focused on specific secure routing protocols in the backbone WMNs with the aim of applying them in HWMNs later on. Several cross-layer secure routing protocols with the combination of routing performance and security were proposed in [7,10] for the backbone WMNs. These protocols combine in a cross-layered approach the different parameters from various layers across the protocol suite. For example routing-layer observations of forwarding behavior and MAC layer to measure the quality of the wireless link in order to select the most reliable path with the highest performance. However, these routing protocols are not suitable for HWMNs due to the ad hoc nature of nodes and their ineffective privacy protection in HWMNs. Khan et al. [7] proposed the Secure Routing Protocol SRPM which is an improved AODV protocol for a backbone WMN. However, SRPM is vulnerable to the attacks launched by legitimate internal mesh nodes and thus cannot provide privacy protection effectively. Islam et al. [11] proposed a secure hybrid wireless mesh protocol (SHWMP) which is a secure extension of HWMP. However, SHWMP is also vulnerable to the attacks launched by legitimate internal mesh routers; an active attacker can compromise and control mesh routers to obtain private user information.

The infrastructure of HWMNs is highly adaptable as opposed to other networks such as the Internet, Wi-Fi, WiMAX, cellular networks or sensor networks. HWMNs are thus considered to be the most applicable architecture for future wireless communications. To make HWMNs function successfully it is imperative to design a routing protocol with security and privacy protection specifically for HWMNs. However, the secure routing protocols for backbone WMNs are not well suited for HWMNs, thus a variety of approaches have been recently proposed for designing secure routing protocols for HWMNs. For instance, Ren et al. [12] proposed PEACE, a novel privacy-enhanced yet accountable security framework for

Please cite this article as: H. Lin et al., A trustworthy and energy-aware routing protocol in software-defined wireless mesh networks, Computers and Electrical Engineering (2016), http://dx.doi.org/10.1016/j.compeleceng.2016.10.015