Computer Networks 54 (2010) 218–230

Contents lists available at ScienceDirect

Computer Networks

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

A global security architecture for operated hybrid WLAN mesh networks

Vincent Toubiana [a,*], Houda Labiod [a], Laurent Reynaud [b], Yvon Gourhant [b]

[a] TELECOM Paristech, LTCI-UMR 5141 CNRS, Institut TELECOM/TELECOM ParisTech/INFRES Department, 46 rue Barrault, 75634 Paris Cedex 13, France
[b] France Telecom R&D, 38-40 rue du Général Leclerc, 92794 Issy Les Moulineaux Cedex 9, France

ARTICLE INFO

Article history:
Available online 28 July 2009

Keywords:
Wireless mesh networks
Hybrid WLAN mesh networks
Ad hoc security
Reactive ad hoc routing
Multipath routing
Authentication
Trust management
Certificate exchange

ABSTRACT

Hybrid Wireless Mesh Network (HWMN) is a new wireless networking paradigm. Unlike traditional wireless networks, in HWMNs, hosts may rely on each other to keep the network connected. Operators and wireless internet service providers are choosing HWMNs to offer Internet connectivity, as it allows fast, easy and affordable network deployments. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we investigate the main security issues focusing on the most vulnerable part of the hybrid WLAN mesh infrastructure which concerns the ad hoc network part. Through our proposed architecture, Security Architecture for Operator's Hybrid WLAN Mesh Network (SATHAME), we identify the new challenges and opportunities posed by this emerging networking environment and explore approaches to secure users, data and communications. From the analysis of strengths and weaknesses of secured routing protocols, we designed a new robust routing structure called MacroGraph (MG). MG structure is extracted from the mesh ad hoc network for each communication to be established between a source and a destination. Especially, MG is a robust structure based on node-disjoint path routing scheme and dynamic trust management that can be adapted to respond to applications' security requirements. We present a performance analysis of our efficient, robust and scalable multipath reactive secured routing protocol. We investigate the behavior of our proposed scheme under two attack scenarios: Packet Dropping and Route Error attacks in dense network configurations.

1. Introduction

Recently, Hybrid Wireless Mesh Networks (HWMNs) have emerged as a promising solution, allowing mobile users to achieve service access in a seamless manner independent of their existence in communication range. In a HWMN any mobile node may have connectivity either directly or via a gateway node to an infrastructure network. This latter network may be an IP network, a 3G wide area wireless network or an IEEE 802.11 wireless local area network. Moreover, hybrid wireless networks may integrate similar or heterogeneous technologies where each mobile node moves between them in an on-demand fashion. A special case of this hybrid configuration can be a WLAN mesh network that combines ad hoc and infrastructures architectures. From a deployment point of view, an operator may have three possibilities: the first one consists to connect a wireless mesh configuration to its existing infrastructure, in the second one, a global hybrid infrastructure including an ad hoc extension is interconnected with the operator architecture and in the third case, the operator deploys a pure ad hoc configuration lonely without any connections to the fixed infrastructure.

In our work, we focus on the deployment of hybrid WLAN mesh configurations because of the widespread of WLAN standards. We actually believe that the second case is the most attractive architecture since it affordably

* Corresponding author. Tel.: +33 650062633.
E-mail addresses: v.toubiana@free.fr (V. Toubiana), labiod@telecom-paristech.fr (H. Labiod), laurent.reynaud@orange-ftgroup. com (L. Reynaud), yvon.gouhrant@orange-ftgroup.com (Y. Gourhant).

1389-1286/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2009.05.016

extends the operator network and let users share personal content with a geographically restricted community composed of direct or indirect neighbors.

Some standardization efforts are paying attention to hybrid wireless networks technology. Standard organizations are actively working on specifications for mesh networking, e.g. IEEE 802.11, IEEE 802.15, IEEE 802.16 and IEEE 802.20. The IEEE 802.11s is concerned with WLAN Mesh networking.

In fact, in most WLAN deployments today, there is a clear distinction between the devices that comprise the network infrastructure and the devices that are clients that simply use the infrastructure to gain access to network resources. The most common WLAN infrastructure devices deployed today use IEEE 802.11a/b/g (and soon 802.11n) access points (APs) that provide a number of services. APs are usually directly connected to a wired network (e.g., 802.3), and simply provide wireless connectivity to client devices rather than utilizing wireless connectivity themselves. Client devices, on the other hand, are typically implemented as simple 802.11 stations (STAs) that must associate with an AP in order to gain access to the network. These simple STAs are dependent on the AP with which they are associated to communicate.

There is no reason, however, that many of the devices under consideration for use in WLANs cannot support much more flexible wireless connectivity. Dedicated infrastructure class devices such as APs should be able to establish peer-to-peer wireless links with neighboring APs to establish a mesh backhaul infrastructure, without the need for a wired network connection to each AP. Moreover, in many cases devices traditionally categorized as clients should also be able to establish peer-to-peer wireless links with neighboring clients and APs in a mesh network. In some cases, these mesh-enabled client devices could even provide the same services as APs to help legacy STAs gain access to the network. In this way, the mesh network extensions proposed blur the lines between infrastructure and client devices in some deployment scenarios. Until now, infrastructure/backbone wireless mesh networks are the most commonly used configurations.

In this paper we consider the hybrid mesh networking paradigm with the assumption that the APs are almost fixed, only clients can be mobile and provide direct connectivity between them.

The main advantages of this kind of configurations are: increased range/coverage and flexibility in use (compared to the basic WLAN standard), reliable performance, high bandwidth for multimedia services, power efficient operation for battery operated devices, density extension support, robustness, dynamic self-organization, self-configuration and self-healing to enable flexible integration, quick deployment, easy maintenance, low cost, high scalability and enhanced network capacity.

In addition to Internet connectivity, HWMN applications are promising in enabling users to access or share various multimedia applications. Specially, combining the two characteristics of a mesh topology and ad hoc capabilities is a very attractive proposition to define innovative applications that can be hosted by mobile users themselves. From an operator's point of view, various applications can be supported such as: P2P file sharing, house monitoring, network gaming, local television/radio broadcasting, instant messaging, localized ads, promotion broadcast and distributed files back-up. Therefore, the development of these emerging applications requires enforcing ad hoc network security.

The design of appropriate security mechanisms, a prerequisite to the adoption and deployment of the cited applications, is a challenging and a complex issue. These security mechanisms should mainly allow stringent authentication and authorization to access network resources and services.

Actually, the ad hoc part remains the Achilles heel of the hybrid WLAN mesh network since many security flaws still unsolved and represent a critical threat to a practical deployment. Some of the main ad hoc inherent problems can be summarized as follows:

- Ad hoc networks rely on wireless multihop transmissions to extend connectivity; a node wanting to send a packet to an indirect neighbor relies on other ad hoc nodes to forward the packet to its destination. Unlike traditional architecture networks where the direct gateway to the existing secured operator infrastructure, is under operator's control, ad hoc connections are routed through many untrusted nodes until they reach their destination. A routing protocol is used to determine the best chain of forwarding nodes in accordance to some performance criteria (bandwidth, delay, energy consumption,...). This routing protocol assumes that every node is willing to take part of collaboration during route establishment and the following data transmission. But for diverse reasons some nodes may refuse to collaborate and reroute traffic through non-optimal routes, or simply refuse to forward data to preserve their local resources.
- With users directly connected to their operators, architecture networks' operators alleviate the authentication issue by sharing, with their user, a secret used to insure mutual authentication. In ad hoc networks, authentication is much more complex as no secret is initially shared by users. As a result, any malicious node can take as many identities as it wants, paying no attention to their eventual assignment to other nodes. Especially, a forwarding node's identity can be spoofed almost instantaneously by a neighbor of it, to reroute traffic or drop it.
- Node mobility involves many topology changes. Huge amount of routing information transits from node to node to maintain an up-to-date vision of the network's topology. With highly dynamic topologies, route changes are frequent and hard to verify. Thus, an attacker can unnoticeably modify routing information and, thereby, degrade network performance, even causing disconnection.

Many attacks are taking advantage of these flaws and disturb the network or squarely cause denial of service. In Hu et al. [1] two main types of attacks are discernible: passive and active attacks. The main passive attacks concern: eavesdropping and traffic analysis. Active attacks