Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Wireless mesh network security: A traffic engineering management approach

Okechukwu E. Muogilim [a,*], Kok-Keong Loo [b], Richard Comley [b]

[a] School of Engineering and Design, Brunel University, UK
[b] School of Engineering and Information Sciences, Middlesex University, UK

ARTICLE INFO

Article history:
Received 9 December 2009
Received in revised form
12 February 2010
Accepted 25 March 2010
Available online 7 April 2010

Keywords:
Traffic engineering
Wireless mesh networks
Security
MPLS
VPN
IPSec

ABSTRACT

The wireless mesh network (WMN) is an emerging multihop, heterogeneous, easily scalable and low cost network. The architecture of the WMN is a connectionless-oriented, mobile and dynamic traffic of routed packets. The mesh infrastructure environment easily forms multiple chains of wireless LANs (WLAN) coupled with the simultaneous multihop transmission of data packets from peripherals via mobile gateways to the wireless cloud. WMN operates as an access network to other communication technologies. This exposes the WMN to numerous security challenges not only in the mesh transmission operation security but also in the overall security against foreign attacks. We surveyed and identified the security vulnerabilities in Internet Protocol (IP) broadband networks, the security challenges in the routing layer of the WMN and explored new concepts to solving security challenges in WMN using traffic engineering (TE) security resolution mechanisms. We analyzed the advantages, comparative strengths and weakness in the use of traffic engineering based on simulation results and evaluations.

1. Introduction

The WMN (Akyildiz et al., 2005; Jun and Sichitiu, 2008; Bruno et al., 2005; Chen et al., 2008) as shown in Fig. 1 comprises the mesh routers, mesh clients and the mesh backbone infrastructure. The mesh clients are mobile and dynamic while the mesh router has static or minimal mobility. These mesh routers form the backbone infrastructure of the WMN, while the mesh clients form two level of nodes operation: at the peripherals and on the access points (AP).

The WMN is similar in operation to the Mobile ad hoc network (MANET) and it employs a multihop routing mechanism from source node to destination node. However, unlike the MANET, WMN uses multiple interfaces and multiple radio frequencies. Furthermore, it uses high speed back-haul network and gateways to optimize network performance and integration with other wireless networks. The mesh routers can also be gateway nodes to the exterior internet cloud or to other networking technologies. These mesh routers operate as bridging points in inter-network and integration with other wireless devices. The AP is a node interface for hosting and retransmission; it provides integration between the mesh client and the mesh backbone infrastructure in WMN. The WMN is self-configuring, self-organizing and self-healing. These qualities make the WMN an excellent wireless access technology for multimedia and community broadband (IEEE 802.16) (Johnston and Walker, 2004).

WMN is an IEEE 802.11s standard (Hiertz et al., 2007) with extensive work being done by workgroups on achieving a standard for its different challenges and protocols. The modifications and adaptations of the ad hoc networks are mostly on the security and routing protocol of WMN. This has led to the adoption of wireless local access network (WLAN, IEEE 802.11i) security and WI-FI protected access (WPA) (Malekzadeh et al., 2005) for WMN. However, improvements by the standardization forums have seen enhancement in the authentication, encryption and integrity of WMN security. Moreover, as most wireless networks are now mostly seen as access-networks to internet or internet service providers (ISP), the Internet Protocol (IP) are easily configurable in achieving a better comprehensive security in the WMN architecture. The WMN unlike the ad hoc networks has commercial qualities, such as it is easily scalable, mobile and dynamic; but these characteristics also create security lapses in the WMN routing operations and MAC layer of the WMN protocol. In 2004, IEEE 802.11i formed a task group (TG) (IEEE Standards, 2004) to prepare and improve the standardization of the WMN. TG was to ratify and prepare the standard amendment to meet the targeted requirement for WMN (IEEE 802.11s). The use of WMN as gateway access to community broadband internet has created an increasing requirement for secure wireless communication

* Corresponding author.
E-mail addresses: Okechukwu.Muogilim@brunel.ac.uk, monxm@yahoo.co.uk (O.E. Muogilim), J.Loo@mdx.ac.uk (K.-K. Loo), R.Comley@mdx.ac.uk (R. Comley).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.03.027

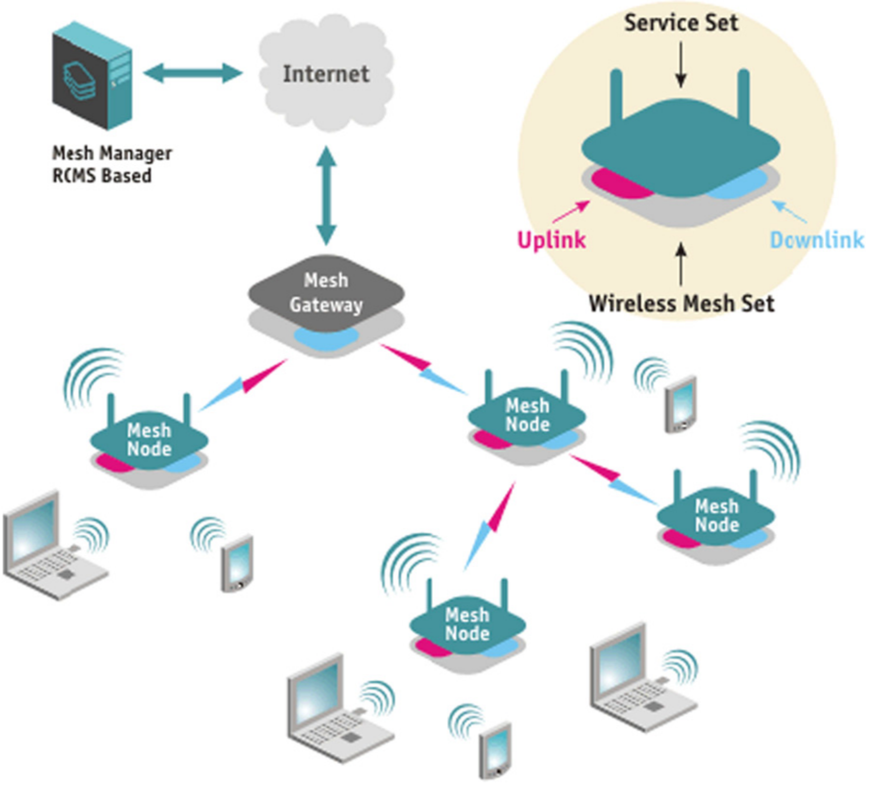

Fig. 1. Wireless mesh network scenario with internet gateways (Wilibox (Wireless Linux in the Box), 2005–2009).

operations. In response to the high commercial demand for multimedia and broadband network operation, due to its low cost and easy operation, highly sensitive application created a necessity for an effective and comprehensive security mechanism in WMN.

WMN operates as access underlying network for broadband. The broadband are dependable and appropriate for many important communication operation and application like voice, data and multimedia services. WMN access for broadband communication networks is both interoperable and easily complementary. Many wireless network applications utilize the broadband network for connection to the internet. WMN, similar to other network applications, makes use of IP addressing and configuration. Most of the transceiver-IP nodes in the WMN are mesh clients and routers with gateway functions operating as access to the internet. Furthermore, the mesh routers act as backbone network, while the mesh clients use medium access control (MAC) addresses for frame transmission among neighborhood network nodes. The IP addresses are enabled by configuration and are either dynamically or statically assigned in the network routing protocol layer. Other layers of the WMN like the transport and session layer protocols transmit routed packets after encapsulation of the data traffics in IP datagram—user datagram protocol (UDP) or transmission control protocol (TCP).

WMN provides a good potential commercial access for community broadband and multimedia networks. The broadband networks are increasingly popular due to the upsurge in internet applications and electronic commerce (e-commerce). WMN is easily scalable over increasing network sizes and provides a low cost and low battery consumption network. It also has an added ease of integration with other wireless and wired networks. The architecture and operation show a hierarchal transmission of traffic and network notification packets through the peripheral (client) nodes through the AP nodes to the backbone wireless mesh router nodes via router gateways to the wireless clouds (internet).

The routing operation of these data traffic over wireless mesh architecture network creates a vulnerable security system caused by the multihop traffic transmission and loose node-to-node data exchange during inter-node authentication mechanism, while routing neighborhood nodes information and exchanging new nodes updates. In addition, the multihop behavioral characteristics of the WMN create challenges on the security of the traffic operations while in transmission through the gateway to the wireless cloud. The dynamic topology updates further expose the whole network security to persistent and corruptible attacks. The reliability and authentication (Khan and Akbar, 2006) of data traffic in WMN during neighborhood nodes exchanges through link state and in routing operations are loose and very insecure. The ease in WMN integration with other wireless nodes and communication networks, like in broadband and multimedia, has also established the necessity for an unyielding privacy protection and security mechanism (Zheng et al., 2005; Salem and Hubaux, 2006; Milanovic et al., 2004).

The distributed-sequenced mechanism in the network's MAC channel frames also creates susceptibility t o attacks while the mobile mesh client nodes and its consequent dynamic topology in the wireless mesh infrastructure also establish the need for more effective, resilient and comprehensive security system in WMN. The constraint in WMN security creates the challenge of possible attacks by invasive worms and viruses, when on attack through simple dynamism of mesh become distributed in the architecture. These attacks compromise the confidentiality and integrity and violate the privacy of the network users. Furthermore, the nodes can also be compromised by the operation of traffic transmission, unverified router information exchange traffic and network notification infiltration. Finally, there are other attacks on the WMN, from physical vandalism to external physical destruction of